KASPERSKY LAB

Kaspersky Anti-Virus 5.0 for Windows Workstations

Guida dell'amministratore

KASPERSKY ANTI-VIRUS® 5.0
FOR WINDOWS WORKSTATIONS

Guida dell'amministratore

© Kaspersky Lab
http://www.kaspersky.com

Data revisione: febbraio 2006

Indice

CAPITOLO 1. KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 7
1.1. Nuove funzioni della versione 5.0 9
1.2. Requisiti di sistema hardware e software 11
1.3. Kit di distribuzione 12
1.3.1. Contratto di licenza 12
1.4. Servizi riservati agli utenti registrati 13
1.5. Legenda 13
CAPITOLO 2. INSTALLAZIONE E RIMOZIONE DELL'APPLICAZIONE 15
2.1. Installazione dell'applicazione 15
2.2. Disinstallazione dell'applicazione 20
2.3. Aggiornamento dalla versione 4.x alla versione 5.0 21
CAPITOLO 3. CONCETTI DI GESTIONE DELL'APPLICAZIONE 22
3.1. Principi di base del concetto di amministrazione 23
3.2. Interfaccia locale 24
3.2.1. L'icona dell'area di notifica 24
3.2.2. Menu di scelta rapida 25
3.2.3. La finestra principale dell'applicazione: struttura generale 26
3.2.3.1. La scheda *Protezione* 27
3.2.3.2. La scheda *Impostazioni* 29
3.2.3.3. La scheda *Assistenza* 30
3.2.4. La finestra Scansione in corso 31
3.2.5. La guida 33
CAPITOLO 4. PROTEZIONE DEL COMPUTER UTILIZZANDO LE IMPOSTAZIONI PREDEFINITE 34
4.1. Impostazioni predefinite 34
4.2. Livelli di protezione antivirus 36
CAPITOLO 5. GESTIONE DELL'APPLICAZIONE TRAMITE L'INTERFACCIA LOCALE 39
5.1. Aggiornamento del database antivirus e dei moduli dell'applicazione 39
5.1.1. Quando scaricare gli aggiornamenti 40

5.1.2. Aggiornamento manuale. Download degli aggiornamenti 40
5.1.3. Configurazione degli aggiornamenti 42
5.1.3.1. Aggiornamento dei moduli dell'applicazione 44
5.1.3.2. Copia degli aggiornamenti nella cartella locale 46
5.1.3.3. Selezione dell'origine degli aggiornamenti 47
5.1.3.4. Configurazione delle impostazioni del server proxy 49
5.1.3.5. Selezione del tipo di database antivirus 50
5.2. Modalità di protezione in tempo reale 52
5.2.1. Scansione del file system 55
5.2.1.1. Selezione del livello di protezione antivirus 56
5.2.1.2. Azioni da eseguire su un oggetto rilevato 58
5.2.2. Scansione della posta 59
5.2.2.1. Selezione del livello di protezione antivirus 61
5.2.2.2. Azioni da eseguire su un oggetto rilevato 63
5.2.3. Scansione della posta di Microsoft Outlook 64
5.2.4. Monitoraggio delle macro 65
5.2.5. Monitoraggio degli script 67
5.2.6. Protezione contro gli attacchi di rete 69
5.3. La modalità di scansione manuale 71
5.3.1. Scansione completa del computer 72
5.3.2. Scansione degli oggetti selezionati 73
5.3.3. Configurazione della scansione manuale 76
5.3.3.1. Selezione del livello di scansione 79
5.3.3.2. Azioni da eseguire su un oggetto rilevato 82
5.3.4. Scansione di archivi 84
5.3.5. Scansione delle unità rimovibili 86
5.4. Elaborazione degli oggetti nocivi rilevati 87
5.5. Monitoraggio dei processi software 91
5.6. Attività utente 93
5.7. Creazione di un elenco di esclusioni 94
5.8. Pianificazione 98
5.9. Lancio di un'attività per conto di un account utente selezionato 101
5.10. Funzionalità supplementari 102
5.10.1. Cartella della quarantena e memoria di backup 103
5.10.1.1. Configurazione dell'archiviazione 103
5.10.1.2. Funzionamento dell'archiviazione in quarantena 105

5.10.1.3. Funzionamento della memoria di backup 107
5.10.2. Uso dei report 109
5.10.3. Gestione della configurazione di Kaspersky Anti-Virus 113
5.10.4. Impostazioni supplementari 114
5.10.5. Configurazione delle richieste di conferma 119
5.10.6. Limitare l'efficienza di Kaspersky Anti-Virus 120
5.10.7. Funzionamento in modalità amministratore e modalità utente 120

CAPITOLO 6. GESTIONE DELL'APPLICAZIONE TRAMITE KASPERSKY ADMINISTRATION KIT 122
6.1. Gestione delle regole 122
6.1.1. Creazione di una regola 122
6.1.2. Visualizzazione e modifica delle impostazioni delle regole 126
6.1.2.1. Visualizzazione delle informazioni sulla regola 127
6.1.2.2. Scansione manuale 128
6.1.2.3. Protezione in tempo reale degli oggetti del file system 131
6.1.2.4. Codici ostili ed esclusioni 134
6.1.2.5. Monitoraggio dei processi software 135
6.1.2.6. Scansione dei messaggi di posta elettronica 136
6.1.2.7. Monitoraggio degli script 139
6.1.2.8. Monitoraggio delle macro 140
6.1.2.9. Protezione contro gli attacchi di rete 142
6.1.2.10. Aggiornamento del database antivirus e dei moduli dell'applicazione 144
6.1.2.11. Gestione delle attività di sistema 145
6.1.2.12. Configurazione dell'archiviazione in quarantena e nella memoria di backup 146
6.1.2.13. Generazione di report sul funzionamento dell'applicazione 147
6.1.2.14. Parametri supplementari 150
6.1.2.15. Visualizzazione dei risultati dell'applicazione delle regole 154
6.2. Gestione delle attività 155
6.2.1. Creazione di un'attività 155
6.2.1.1. Creazione di un'attività locale 156
6.2.1.2. Creazione di un'attività di gruppo 162
6.2.1.3. Creazione di un'attività globale 162
6.2.2. Visualizzazione e modifica delle impostazioni delle attività e monitoraggio del loro funzionamento 163
6.2.3. Esecuzione e interruzione delle attività 164

6.3. Configurazione delle impostazioni dell'applicazione 164
6.3.1. Visualizzazione delle informazioni sull'applicazione 166
6.3.2. Impostazioni supplementari dell'applicazione 168
6.3.3. Uso delle aree di archiviazione di quarantena e backup 169
6.3.4. Visualizzazione delle informazioni sulle chiavi di licenza 171
6.3.5. Configurazione dei parametri per la generazione dei report 171
CAPITOLO 7. TEST DI FUNZIONAMENTO DI KASPERSKY ANTI-VIRUS 172
7.1. "Virus" di prova EICAR e sue modifiche 172
7.2. Prova del corretto funzionamento di Kaspersky Anti-Virus 174
CAPITOLO 8. GESTIONE DELLE CHIAVI DI LICENZA 176
8.1. Gestione delle chiavi utilizzando l'interfaccia locale 177
8.2. Gestione delle chiavi di licenza tramite l'interfaccia di Kaspersky Administration Kit 180
CAPITOLO 9. GESTIONE DELL'APPLICAZIONE DALLA RIGA DI COMANDO 181
9.1. Scansione degli oggetti selezionati 182
9.2. Scansione completa 184
9.3. Avvio degli aggiornamenti 185
9.4. Ripristino della versione precedente del database antivirus 186
9.5. Modalità di protezione in tempo reale 187
9.6. Avvio dell'applicazione 188
9.7. Arresto dell'applicazione 188
9.8. Gestione delle attività 189
9.9. Importazione/esportazione delle impostazioni 191
9.10. Aggiunta di una chiave di licenza 191
CAPITOLO 10. DOMANDE FREQUENTI 192
APPENDICE A. CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA 199
APPENDICE B. GLOSSARIO 201
APPENDICE C. KASPERSKY LAB 208
C.1. Altri prodotti Kaspersky Lab 209
C.2. Recapiti 215
APPENDICE D. CONTRATTO DI LICENZA 216

CAPITOLO 1. KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS

Kaspersky Anti-Virus® for Windows Workstations (che nel resto del documento verrà chiamato Kaspersky Anti-Virus) è progettato per proteggere le workstation da virus e malware.

Nell'applicazione sono state implementate le seguenti funzionalità:

- **Protezione del computer da virus e malware** - rilevamento ed eliminazione del malware dal computer. Sono disponibili due modalità operative, che possono essere utilizzate separatamente o in contemporanea:
    - **Protezione del computer in tempo reale** - vengono esaminati alla ricerca di virus tutti gli oggetti eseguiti, aperti o salvati sul computer.
    - **Protezione manuale del computer** - vengono esaminati alla ricerca di virus sia il computer che i singoli file e le singole unità e cartelle. Tale scansione può essere lanciata manualmente, oppure pianificata per l'esecuzione automatica ad intervalli specifici.
- **Ripristino dopo l'attacco da parte di un virus**. La scansione completa e la disinfezione utilizzano le impostazioni raccomandate dagli esperti di Kaspersky Lab, e consentono di identificare tutti i virus che hanno infettato i dati sul computer.
- **Scansione e disinfezione della posta in arrivo ed in uscita** - analisi e disinfezione antivirus di tutta la posta in arrivo ed in uscita in modalità di tempo reale[1]. Inoltre, l'applicazione consente la scansione e la disinfezione manuale dei database di posta dei client di posta elettronica[2].
- **Protezione del computer contro gli attacchi di rete** - analisi di tutti i dati ricevuti sul computer dell'utente dalla rete (LAN e Internet), per identificare gli attacchi dalla rete. Una volta rilevato un attacco di rete,

[1] L'applicazione esamina tutta la posta inviata e ricevuta tramite Microsoft Outlook, a prescindere dai protocolli di posta utilizzati, e tutta la posta inviata e ricevuta da qualsiasi altro programma utilizzando i protocolli SMTP e POP3.

[2] Kaspersky Anti-Virus esamina i database di posta di qualsiasi programma client di posta elettronica, ma disinfetta solo i database di Microsoft Outlook e Microsoft Outlook Express.

verrà offerta la protezione necessaria bloccando il computer di provenienza dell'attacco. Inoltre, l'applicazione utilizzerà la modalità invisibile che consente la ricezione di dati esclusivamente dai computer partecipanti allo scambio di dati avviato dall'utente.

- **Aggiornamento del database antivirus, del database degli attacchi di rete e dei moduli dell'applicazione** - aggiornamento del database anti-virus e del database degli attacchi di rete con informazioni su nuovi virus ed attacchi e sui nuovi metodi da utilizzare per disinfettare gli oggetti infetti da tali virus e malware, nonché aggiornamento dei moduli dell'applicazione (se tale funzione è abilitata). Gli aggiornamenti vengono scaricati dal server di aggiornamento di Kaspersky Lab specificato dall'utente, oppure da una cartella apposita locale o di rete.

- **Raccomandazioni per l'impostazione ed il funzionamento dell'applicazione** - diversi suggerimenti e varie raccomandazioni dagli esperti di Kaspersky Lab per configurare l'applicazione in modo da garantire una protezione antivirus ottimale durante l'utilizzo di Kaspersky Anti-Virus.

  Quando vengono rilevati oggetti pericolosi, se il database antivirus non è stato aggiornato o non è stata eseguita la scansione completa del computer da molto tempo, la finestra principale di Kaspersky Anti-Virus raccomanda l'esecuzione di alcune attività con le relative spiegazioni.

  Grazie alla vasta esperienza pratica accumulata nel settore della protezione antivirus e all'analisi del feedback che il nostro Servizio di assistenza tecnica ha ricevuto dagli utenti, gli specialisti di Kaspersky Lab hanno fatto del loro meglio per configurare l'applicazione in modo da assicurare un funzionamento ottimale. Le impostazioni antivirus raccomandate dai nostri esperti vengono applicate subito dopo aver installato e lanciato l'applicazione.

- **Utilizzo di diversi profili di configurazione dell'applicazione** - creazione ed utilizzo di speciali file di configurazione - i *profili* - che memorizzano le impostazioni dell'applicazione. Specificando le impostazioni dell'applicazione e salvandole nei profili, è possibile modificare con facilità le impostazioni di Kaspersky Anti-Virus. Quindi, è possibile ad esempio configurare l'applicazione in modo che utilizzi la modalità di protezione in tempo reale o che esegua solo l'attività di scansione manuale, ed utilizzare tali configurazioni solo quando richiesto. Kaspersky Anti-Virus consente inoltre di tornare alle impostazioni raccomandate per l'applicazione in qualsiasi momento.

- **Utilizzo dell'applicazione in due modalità operative** - è possibile utilizzare l'applicazione in modalità *utente* o *amministratore*. In modalità utente, è disponibile solo la funzionalità di base di Kaspersky Anti-Virus, mentre non è possibile modificare le impostazioni dell'applicazione o

disabilitare la protezione antivirus. La modalità amministratore consente invece di accedere a tutte le funzioni per gestire l'applicazione.

- **Mettere gli oggetti in quarantena** - trasferimento degli oggetti potenzialmente infettati da virus o loro modifiche in una memoria speciale di archiviazione, dove possono essere disinfettati, eliminati, ripristinati nella cartella originaria o inviati agli esperti di Kaspersky Lab per l'analisi. I file messi in quarantena vengono memorizzati in un formato speciale che non presenta rischi.
- **Creazione di copie di backup degli oggetti** - creazione di copie speciali di backup degli oggetti in una memoria dedicata, prima di cercare di disinfettarli o eliminarli. Tali copie vengono create per i casi in cui fosse necessario ripristinare l'oggetto originale, se contenente informazioni importanti, oppure per ripristinare la situazione di quando ha avuto luogo l'infezione. Le copie vengono memorizzate in un formato speciale che non presenta rischi.
- **Creazione di report** - tutti i risultati del funzionamento di Kaspersky Anti-Virus vengono memorizzati in diversi report. Il report dettagliato riguardante i risultati della scansione comprende le informazioni statistiche generali riguardanti gli oggetti esaminati e contiene informazioni sulle impostazioni utilizzate per eseguire le attività, sull'ordine della scansione e sull'elaborazione di ciascun oggetto specifico. I rapporti vengono creati anche per i risultati degli aggiornamenti e per il funzionamento della modalità di protezione in tempo reale.
- **Gestione centralizzata in remoto dell'applicazione** - l'applicazione può essere gestita tramite il sistema di amministrazione centralizzata Kaspersky Administration Kit 5.0.

Alcune funzioni di Kaspersky Anti-Virus sono disponibili dalla riga di comando (per dettagli, vedere il Capitolo 9 a pagina 181).

1.1. Nuove funzioni della versione 5.0

Le differenze tra la Versione 5.0 di **Kaspersky Anti-Virus for Windows Workstations** e la precedente versione 4.x sono le seguenti:

- *L'utilizzo delle tecnologie di accelerazione della scansione: iChecker™ e iStreams™.* Kaspersky Anti-Virus non riesamina più gli oggetti che sono già stati analizzati durante una scansione precedente e da allora non sono stati modificati, non solo nella modalità di protezione in tempo reale

ma anche durante una scansione manuale. Questa funzione consente di accelerare notevolmente il funzionamento dell'applicazione.

- *Scansione e disinfezione della posta* inviata o ricevuta tramite qualsiasi applicazione client di posta utilizzando i protocolli SMTP e POP3. Le versioni precedenti garantivano la protezione antivirus della posta solo per Microsoft Outlook.

- *Disinfezione degli archivi infetti*. Kaspersky Anti-Virus consente di disinfettare i file infetti contenuti in archivi *zip*, *arj*, *cab*, *rar*, *lha* e *ice*. Le versioni precedenti dell'applicazione prevedevano solo il rilevamento dei file infetti negli archivi e la disinfezione degli oggetti infetti contenuti negli archivi zip.

Kaspersky Anti-Virus esamina gli archivi a più volumi dei formati suddetti e gli archivi autoestraenti, ma non li disinfetta.

- *La velocità del processo di aggiornamento del database antivirus è stata aumentata* facendo sì che venga utilizzato il server di aggiornamento di Kaspersky Lab più vicino alla posizione geografica dell'utente. È stata implementata la capacità di ricevere la parte rimanente degli aggiornamenti in caso di disconnessione.

- *Protezione contro gli attacchi di rete*. Questa versione di Kaspersky Anti-Virus garantisce la protezione del computer contro gran parte dei più comuni attacchi di rete e dei pirati informatici.

- *Interfaccia intuitiva*. L'applicazione viene ora implementata come un singolo programma, mentre le versioni precedenti erano costituite da un insieme di programmi che eseguivano funzioni individuali di protezione antivirus. Questo nuovo approccio consente una gestione semplice ed intuitiva delle funzioni più importanti di Kaspersky Antivirus.

- *Impostazioni raccomandate e suggerimenti degli esperti*. In questa versione, le impostazioni raccomandate dagli esperti di Kaspersky Lab vengono utilizzate come impostazioni predefinite per semplificare l'utilizzo del programma. In gran parte dei casi, non è necessario configurare l'applicazione prima dell'uso. Nelle situazioni in cui la protezione antivirus è impostata al livello più basso, l'applicazione visualizza un messaggio corrispondente e suggerisce diverse maniere per aumentare il grado di protezione.

- *Gestione dei profili di funzionamento dell'applicazione*. Le impostazioni dell'applicazione possono essere salvate in file speciali per utilizzarle in seguito. Se non si è soddisfatti delle impostazioni di Kaspersky Anti-Virus, configurarlo come meglio si ritiene opportuno e salvare questa configurazione in un *profilo*.

- *Rinnovo della licenza per l'applicazione*. Kaspersky Anti-Virus 5.0 consente di installare la chiave di licenza per rinnovare la licenza dell'applicazione.
- *Invio di oggetti a Kaspersky Lab per l'analisi.* Ora è possibile inviare gli oggetti possibilmente infetti rilevati da Kaspersky Anti-Virus ed i file che si sospettano essere infetti a Kaspersky Lab, per l'analisi.
- *I database di posta infetti non possono essere eliminati*. Ora Kaspersky Anti-Virus non elimina i database di posta infetti. Tuttavia, è sempre possibile eliminare tali oggetti manualmente.
- *Capacità di creare l'elenco di processi attendibili*. Kaspersky Anti-Virus non controlla le attività dei processi attendibili nella modalità di protezione in tempo reale.
- *Funzione di gestione delle impostazioni di Kaspersky Anti-Virus protetta da password*. È possibile impostare una password che verrà richiesta per passare dalla modalità utente a quella amministratore. In modalità utente, non è possibile modificare le impostazioni dell'applicazione, disabilitare la protezione in tempo reale o chiudere Kaspersky Anti-Virus.

1.2. Requisiti di sistema hardware e software

Per garantire un funzionamento normale di **Kaspersky Anti-Virus for Windows Workstations**, la workstation deve soddisfare i seguenti requisiti:

Requisiti generali:

- 50 Mb di spazio libero sul disco;
- Unità CD-ROM (per l'installazione di Kaspersky Anti-Virus da CD);
- Microsoft Internet Explorer 5.5 o superiore (per poter aggiornare il database antivirus ed i moduli dell'applicazione da Internet).

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- processore Intel Pentium® 300 MHz o superiore;
- 64 MB di RAM.

Microsoft Windows 2000 Professional (Service Pack 2 o superiore), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 o superiore):

- processore Intel Pentium® 300 MHz o superiore;
- 128 MB di RAM.

1.3. Kit di distribuzione

È possibile acquistare il software presso i nostri distributori (confezione "retail") o presso uno dei nostri negozi web (per esempio su www.kaspersky.com, sezione **E-Store**).

La confezione "retail" contiene:

- una busta sigillata con un CD di installazione contenente i file dell'applicazione;
- un manuale dell'utente;
- una chiave di licenza inclusa nel pacchetto di distribuzione o memorizzata su un disco floppy speciale;
- una scheda di registrazione indicante il numero di serie del prodotto;
- un contratto di licenza.

Leggere attentamente il contratto di licenza prima di aprire la busta contenente il CD.

Se il prodotto viene acquistato da un negozio Web, esso verrà scaricato dal sito Kaspersky Lab ed il pacchetto di distribuzione conterrà anche questa guida. La chiave di licenza viene inclusa nel file di installazione oppure inviata per posta elettronica una volta ricevuto il pagamento.

1.3.1. Contratto di licenza

Il contratto di licenza costituisce un accordo avente valore legale stipulato tra il cliente e Kaspersky Lab e contiene i termini e le condizioni di utilizzo del software acquistato.

Si raccomanda di leggere attentamente il Contratto di licenza!

Se non si accettano i termini del Contratto di licenza, è possibile restituire la confezione contenente Kaspersky Anti-Virus al distributore dal quale è stato effettuato l'acquisto; l'importo versato per l'iscrizione sarà interamente rimborsato, sempre che la busta contenente il CD d'installazione non sia stata aperta.

Aprendo la busta sigillata contenente il CD d'installazione o installando il prodotto sul computer si accettano i termini e le condizioni del Contratto di licenza.

1.4. Servizi riservati agli utenti registrati

Kaspersky Lab offre ai propri utenti autorizzati una vasta gamma di servizi che aiutano a massimizzare l'efficienza di Kaspersky Anti-Virus.

Acquistando un'iscrizione, si diventa utenti registrati del software e si acquisisce il diritto ai seguenti servizi per l'intero periodo di iscrizione:

- aggiornamenti software;
- consulenze telefoniche o via posta elettronica su problemi di installazione, configurazione e uso del software;
- comunicazioni sulla disponibilità di nuovi prodotti software di Kaspersky Lab e sui nuovi virus in diffusione nel mondo (questo servizio è riservato agli utenti iscritti alla newsletter di Kaspersky Lab).

Non vengono offerte consulenze per problemi legati alla funzionalità del sistema operativo o all'uso di diverse tecnologie.

1.5. Legenda

In questo documento vengono utilizzate diverse icone e caratteristiche di formattazione, in funzione dell'obiettivo e del significato del testo. La tabella seguente elenca le convenzioni utilizzate nel testo.

Caratteristica di formattazione	Scopo
Carattere grassetto	Titoli dei menu, voci dei menu, finestre, finestre di dialogo e relative voci, ecc.

Caratteristica di formattazione	Scopo
Nota.	Informazioni supplementari, note.
Attenzione!	Informazioni che richiedono particolare attenzione
Per eseguire l'azione descritta 1. Step 1. 2. …	Descrizione dei passaggi consecutivi e delle azioni possibile da parte dell'utente
Attività, esempio	Descrizione di un problema, esempio delle capacità dell'applicazione

CAPITOLO 2. INSTALLAZIONE E RIMOZIONE DELL'APPLICAZIONE

Esistono due possibilità per l'installazione di **Kaspersky Anti-Virus 5.0 for Windows Workstations**: installazione locale e remota (tramite il sistema di amministrazione centralizzata Kaspersky Administration Kit). Questo manuale descrive la modalità di installazione locale di Kaspersky Anti-Virus su una workstation. Per informazioni sull'installazione remota dell'applicazione, vedere la guida di Kaspersky Administration Kit 5.0.

2.1. Installazione dell'applicazione

Si consiglia di chiudere tutte le applicazioni in esecuzione sul computer prima di installare Kaspersky Anti-Virus.

Per installare l'applicazione, lanciare il file eseguibile incluso nel pacchetto di distribuzione.

Il processo d'installazione tramite il pacchetto d'installazione ricevuto via internet è del tutto analogo all'installazione tramite CD.

Il programma d'installazione opera interattivamente. Ciascuna finestra contiene un insieme di pulsanti che controllano il processo d'installazione. Lo scopo di questi pulsanti è descritto brevemente di seguito:

- **Avanti >** - conferma l'azione e procede allo step successivo del processo d'installazione.
- **< Indietro** - torna allo step precedente del processo d'installazione.
- **Annulla** - termina il processo d'installazione.
- **Fine** - completa il processo d'installazione.

Ciascuno step dell''installazione del programma è trattato in dettaglio di seguito.

Fase 1. Verifica della versione del sistema operativo installato

Prima di iniziare l'installazione dell'applicazione, verrà eseguito un controllo per verificare che il sistema operativo e i Service Pack installati sul computer soddisfino i requisiti software per l'installazione di Kaspersky Anti-Virus.

Se uno qualsiasi dei requisiti non è soddisfatto, verrà visualizzata la relativa notifica sullo schermo. Si consiglia si installare il software e i Service Pack richiesti utilizzando il servizio **Windows Update** (o altro servizio adeguato), prima di installare Kaspersky Anti-Virus.

Fase 2. Ricerca di altri software antivirus

Durante questa fase, verrà eseguita una ricerca di altri software antivirus installati sul computer, compresi altri software di Kaspersky Lab, in grado di causare conflitti se utilizzati in combinazione con Kaspersky Anti-Virus.

Se sul computer viene rilevata una versione precedente di Kaspersky Anti-Virus (ad esempio, la versione 4.5), l'applicazione verrà automaticamente aggiornata dalla versione 4.x alla versione 5.0 (per dettagli, vedere la sezione 2.3 a pagina 21).

Se viene rilevata una chiave di licenza per Kaspersky Anti-Virus for Windows Workstations 4.x, la finestra di dialogo d'installazione della chiave di licenza (vedere lo Fase 8. a pagina 18), che viene visualizzata durante l'installazione, conterrà informazioni su tale chiave. È possibile utilizzare questa chiave o selezionarne un'altra per utilizzare l'applicazione.

Se viene rilevato software antivirus di altri produttori installato sul computer, verrà visualizzato un messaggio che ne consiglia la disinstallazione prima di installare Kaspersky Anti-Virus.

Si consiglia di disinstallare tale software. Per fare ciò, scegliere il pulsante **No** per terminare il processo d'installazione. Quindi, disinstallare le applicazioni come richiesto e lanciare nuovamente il file eseguibile.

Kaspersky Lab sconsiglia l'installazione di più software antivirus su un computer, poiché ciò può causare conflitti durante il loro utilizzo

Se viene rilevata una copia di Kaspersky Anti-Virus 5.0 for Windows Workstations installata sul computer, verrà visualizzato il seguente messaggio sullo schermo. Se si procede con l'installazione, la versione installata in precedenza verrà aggiornata da questa copia dell'applicazione.

Se si aggiorna la versione 5.0, la finestra d'installazione della chiave di licenza (vedere lo Fase 8. a pagina 18) non conterrà informazioni sulla chiave, ma l'applicazione utilizzerà la chiave installata in precedenza.

Fase 3. Finestra iniziale del programma d'installazione

Se non è stato rilevato nessun altro software antivirus sul computer, sullo schermo verrà visualizzata la finestra iniziale per comunicare l'inizio del processo d'installazione di Kaspersky Anti-Virus.

Per procedere con l'installazione, scegliere **Avanti**>. Per annullare l'installazione, scegliere il pulsante **Annulla**.

Fase 4. Lettura del contratto di licenza

La finestra di dialogo **Contratto di licenza** riporta il testo del contratto di licenza. Leggerlo e scegliere **Accetto** se si accettano i termini e le condizioni del contratto. Per uscire dal programma di installazione, scegliere il pulsante **Annulla**.

Fase 5. Immissione delle informazioni sull'utente

Immettere le informazioni richieste nella finestra di dialogo **Informazioni sul cliente**. Immettere il proprio nome nel campo **Nome utente**, e il nome dell'organizzazione nel campo **Azienda** Per impostazione predefinita, la finestra conterrà le informazioni ottenute dal registro di Windows.

Fase 6. Lettura di importanti informazioni sull'applicazione

In questa fase verranno visualizzate importanti informazioni relative all'applicazione. Questa finestra comunica le funzioni principali di Kaspersky Anti-Virus, le particolarità del suo funzionamento, e così via.

Per procedere alla fase successiva dell'installazione, scegliere **Avanti >**.

Fase 7. Utilizzo delle tecnologie di Kaspersky Lab

Durante questa fase del processo di installazione di Kaspersky Anti-Virus, sarà necessario decidere se l'applicazione dovrà utilizzare o meno le seguenti tecnologie:

Protezione in tempo reale contro gli attacchi di rete - tecnologia utilizzata per proteggere il computer dagli attacchi dei pirati informatici. Questa tecnologia protegge il computer dagli attacchi provenienti dalla rete, previene la corruzione o il furto dei dati ed impedisce l'accesso non autorizzato ad essi. Per impostazione predefinita, la protezione in tempo reale dagli attacchi di rete è disabilitata. Per abilitare la protezione in

tempo reale, selezionare la casella **Usa la protezione in tempo reale contro gli attacchi di rete**. È possibile abilitare o disabilitare la protezione in tempo reale dagli attacchi di rete successivamente, durante l'utilizzo del programma (vedere la sezione 5.2.6 a pagina 69)

Tecnologia iStreams™ - tecnologia di accelerazione della scansione antivirus (per una descrizione dettagliata di questa tecnologia, vedere Appendice B a pagina 201). Per disabilitare l'utilizzo di questa tecnologia, deselezionare la casella **Usa la tecnologia iStreams**™.

Questa tecnologia può essere utilizzata solo su file system NTFS.

Se si disabilita l'utilizzo della tecnologia iStreams, sarà necessario reinstallare Kaspersky Anti-Virus per abilitarla in seguito.

Per procedere con l'installazione, scegliere **Avanti**>.

Fase 8. Installazione della chiave di licenza.

È necessario selezionare la chiave di licenza utilizzata da Kaspersky Anti-Virus per verificare il Contratto di licenza e determinarne la validità; la chiave di licenza viene selezionata tramite la finestra **Chiave di licenza**.

La chiave di licenza è una "chiave" personale che contiene tutte le informazioni di servizio richieste per la funzionalità completa dell'applicazione, vale a dire:

- informazioni di assistenza (chi fornisce assistenza e come ottenerla);
- il nome, il numero e la data di scadenza della licenza.

Per installare una nuova chiave di licenza,

1. Scegliere il pulsante **Sfoglia** e passare alla cartella contenente la chiave di licenza:
   - Se Kaspersky Anti-Virus è stato acquistato in confezione (confezione "retail"), la chiave di licenza sarà scritta su un dischetto floppy. Sarà necessario inserire il dischetto nell'unità e selezionare l'unità stessa per accedere al dischetto.
   - Se la licenza è stata acquistata on-line, salvare il file della chiave di licenza ricevuto per posta elettronica in qualsiasi cartella sul disco rigido del computer. Quindi, passare a tale cartella.

La cartella selezionata visualizzerà un elenco delle chiavi di licenza disponibili.

2. Selezionare il file chiave di licenza richiesto (con estensione **.key**) e scegliere il pulsante **Apri**.

A questo punto, l'installazione guidata visualizzerà informazioni generali sulla licenza ed il percorso al file.

Per procedere con l'installazione dell'applicazione, scegliere il pulante **Avanti >**.

Se, al momento dell'installazione, non si dispone ancora della chiave di licenza (ad esempio perché è stata ordinata a Kaspersky Lab via Internet, ma non è ancora stata ricevuta), la chiave potrà essere installata in seguito, quando si esegue l'applicazione, oppure tramite una speciale utility di installazione della chiave di licenza (vedere il Capitolo 8 a pagina 176) Si noti che non è possibile utilizzare Kaspersky Anti-Virus senza chiave di licenza.

Fase 9. Selezione della cartella di installazione

La cartella di installazione di Kaspersky Anti-Virus può essere selezionata nella finestra di dialogo **Scegliere la cartella di destinazione**. Per selezionare la cartella utilizzare il pulsante **Sfoglia**.

È possibile ripristinare il percorso alla cartella di installazione predefinita utilizzando il pulsante Ripristino; il percorso predefinito è: **<Unità>\Programmi\Kaspersky Lab\Kaspersky Anti-Virus 5.0 for Windows Workstations**.

La finestra che si apre tramite il pulsante Utilizzo disco contiene informazioni relative allo spazio disponibile e a quello richiesto per l'installazione sulle unità logiche della workstation.

Per procedere con l'installazione, scegliere il pulsante **Installa** . Ciò avvierà il processo di copia dei file di Kaspersky Anti-Virus sul computer.

Fase 10. Completamento dell'installazione

La finestra **Installazione completata** visualizza informazioni relative al completamento dell'installazione di Kaspersky Anti-Virus sul computer.

Per completare l'installazione dell'applicazione, è necessario registrare alcuni servizi nel sistema, quindi verrà richiesto di riavviare il computer. Il riavvio del sistema è ASSOLUTAMENTE NECESSARIO per completare correttamente l'installazione. Scegliere **Sì** nella finestra che si aprirà per riavviare subito il computer, oppure **No** per riavviare in seguito.

Kaspersky Anti-Virus riavvierà automaticamente il sistema.

Dopo l'installazione di Kaspersky Anti-Virus:

- L'icona dell'applicazione verrà visualizzata nell'area di notifica.
- Verranno aggiunti collegamenti all'applicazione nel menu principale di Windows (**Start → Tutti i programmi→ Kaspersky Anti-Virus 5.0 for Windows Workstations**).

2.2. Disinstallazione dell'applicazione

Se per qualsiasi motivo si desidera disinstallare Kaspersky Anti-Virus, scegliere **Start → Tutti i programmi → Kaspersky Anti-Virus 5.0 for Windows Workstations → Disinstalla Kaspersky Anti-Virus**, oppure utilizzare lo strumento standard di Windows **Installazione applicazioni** dal Pannello di controllo.

Se l'applicazione è controllata tramite Kaspersky Administration Kit con abilitazione della password di protezione per prevenirne la disinstallazione non autorizzata (vedere la sezione 6.1.2.14 a pagina 150), è necessario digitare la password prima della rimozione.

Verrà quindi richiesto di confermare la rimozione. Per avviare la procedura di disinstallazione, fare clic su **OK**. Si aprirà quindi una finestra che consente di scegliere se rimuovere o conservare gli oggetti in quarantena o nella memoria di backup, i report e i file delle chiavi di licenza.

A questo punto si avvierà il processo di eliminazione dei file dell'applicazione dal disco rigido del computer.

Se il programma di disinstallazione rileva la presenza di file che possono essere utilizzati da altre applicazioni, si apre una finestra di dialogo che chiede conferma per eliminare tali file. Fare clic sul pulsante **Sì** per eliminarli.

Al termine della disinstallazione dell'applicazione, viene richiesto di riavviare la workstation. Selezionare l'opzione desiderata e fare clic sul pulsante **Fine**.

2.3. Aggiornamento dalla versione 4.x alla versione 5.0

Prima di iniziare l'aggiornamento di Kaspersky Anti-Virus si consiglia di elaborare gli oggetti in quarantena e nella memoria di backup.

Per aggiornare la versione 4.x di Kaspersky Anti-Virus for Windows Workstations alla versione 5.0, lanciare il file eseguibile. La versione precedente di Kaspersky Anti-Virus esistente verrà rimossa durante il processo d'installazione.

Al termine del processo d'installazione, è necessario riavviare il sistema operativo.

Si noti che, durante l'aggiornamento, le impostazioni di Kaspersky Anti-Virus 4.x non saranno salvate. È possibile utilizzare le impostazioni raccomandate predefinite o riconfigurare l'applicazione.

In caso di installazione remota dell'applicazione tramite Kaspersky Administration Kit (vedere la guida di Kaspersky Administration Kit 5.0), la versione 4.x sarà aggiornata automaticamente alla versione 5.0: la versione esistente di Kaspersky Anti-Virus verrà rimossa e il computer remoto riavviato.

CAPITOLO 3. CONCETTI DI GESTIONE DELL'APPLICAZIONE

Kaspersky Anti-Virus viene installato su una workstation e può essere controllato localmente o in remoto, tramite Kaspersky Administration Kit (se il computer fa parte del sistema di controllo centralizzato).

Esistono diverse categorie di utenti di Kaspersky Anti-Virus:

- L'*Utente della workstation* è l'utente della workstation su cui è installato Kaspersky Anti-Virus.
- L'*Amministratore della sicurezza antivirus* (d'ora in poi chiamato "amministratore") è responsabile della gestione locale di Kaspersky Anti-Virus.
- L'*Amministratore della rete logica* controlla il funzionamento di Kaspersky Anti-Virus tramite il sistema di amministrazione centralizzata in remoto di Kaspersky Administration Kit.

Ad ogni categoria di utenza è assegnata la propria interfaccia, che fornisce l'accesso a tutte le funzioni del software che la categoria stessa può utilizzare, in base ai rispettivi privilegi.

L'**Interfaccia utente** è ottimizzata per l'efficienza e la semplicità e consente di eseguire le seguenti attività:

- visualizzazione delle informazioni di stato relative alla protezione antivirus;
- esecuzione delle attività di scansione degli oggetti del file system;
- aggiornamento del database antivirus e dei moduli dell'applicazione (se tale funzione è stata abilitata dall'amministratore);
- visualizzazione dei log di esecuzione delle attività e degli eventi;
- visualizzazione del contenuto della quarantena e della memoria di backup, ed invio dei file in quarantena a Kaspersky Lab per l'analisi.

Oltre alle attività utente, l'**interfaccia amministratore** estesa consente una configurazione semplice e flessibile del funzionamento di Kaspersky Anti-Virus per l'esecuzione delle seguenti attività:

- modifica delle impostazioni delle attività di protezione antivirus in tempo reale;
- creazione, gestione e pianificazione delle attività di scansione degli oggetti del file system e di aggiornamento;

Se viene utilizzata l'amministrazione centralizzata tramite Kaspersky Administration Kit, l'applicazione è controllata in remoto da un computer su cui è installata la *Consolle di amministrazione*.

La consolle di amministrazione è un'**interfaccia standard integrata nell'MMC** che consente all'amministratore della rete logica di eseguire le seguenti operazioni:

- installazione in remoto di Kaspersky Anti-Virus sui computer client;
- aggiornamento del database antivirus e dei moduli dell'applicazione;
- gestione delle regole e delle attività sui computer client;
- installazione delle chiavi di licenza sui computer client;
- visualizzazione dei report relativi al funzionamento dell'applicazione sui computer client.

Se si desidera controllare l'applicazione tramite Kaspersky Administration Kit, sarà necessario installare l'agente di rete sul computer client; esso consente alla workstation di interagire con il server di amministrazione (per maggiori dettagli, vedere la guida di Kaspersky Administration Kit 5.0).

Per maggiori dettagli sul concetto di amministrazione centralizzata, vedere la guida dell'amministratore di Kaspersky Administration Kit 5.0.

3.1. Principi di base del concetto di amministrazione

Se il programma è amministrato localmente, la protezione fornita da Kaspersky Anti-Virus viene configurata dall'amministratore modificando le impostazioni e le attività dell'applicazione.

Un'**attività** è un'azione specifica eseguita dall'applicazione. Le attività sono suddivise in tipi, secondo il loro scopo (attività di scansione completa, attività di aggiornamento del database antivirus e dei moduli dell'applicazione, ecc.). A ciascun'attività viene applicato un insieme di parametri (*impostazioni dell'attività*) per la sua esecuzione, vale a dire:

Impostazioni dell'applicazione - un insieme di parametri supplementari definiti per il funzionamento dell'applicazione, tra cui i parametri per la quarantena, la memoria di backup, il servizio di generazione dei report, ecc.

Se si utilizza l'amministrazione centralizzata tramite Kaspersky Administration Kit, l'amministratore definisce le impostazioni e le attività per l'applicazione installata su un computer remoto della rete.

Una funzione specifica dell'amministrazione centralizzata è la disposizione dei computer in gruppi e la modifica delle loro impostazioni creando e definendo regole di gruppo.

Una **Regola** è un insieme di impostazioni dell'applicazione riguardanti il suo funzionamento in un gruppo di rete logica ed un insieme di restrizioni per ridefinire tali parametri durante la configurazione dell'applicazione o di un'attività.

Una regola include i parametri richiesti per la configurazione completa della funzionalità dell'applicazione, e comprende sia le impostazioni dell'applicazione che le impostazioni per tutti tipi di attività, tranne i parametri che devono essere definiti ogni volta che viene avviata un'attività specifica.

3.2. Interfaccia locale

L'interfaccia di Kaspersky Anti-Virus è intuitiva e facile da utilizzare. Questa sezione contiene una descrizione dettagliata dei suoi elementi principali: l'icona dell'area di notifica, il menu di scelta rapida, la finestra principale ed alcune finestre di assistenza.

3.2.1. L'icona dell'area di notifica

Una volta lanciata l'applicazione, l'icona dell'applicazione viene visualizzata nell'area di notifica; il suo aspetto varia secondo lo stato della protezione antivirus, indicando se la protezione in tempo reale è abilitata o se è stata avviata una scansione manuale.

Se l'icona è abilitata (colore rosso), ciò significa che tutti i file sul computer sono controllati da Kaspersky Anti-Virus. Se l'icona non è abilitata (colore grigio), ciò significa che la protezione in tempo reale è disabilitata (per esempio, se la protezione in tempo reale è stata sospesa o se è stata disabilitata la funzione di protezione in tempo reale dei file).

Se è in corso una scansione completa del computer o di un singolo file o un'analisi in modalità di tempo reale di un oggetto, l'icona nell'area di notifica lampeggia. La scansione della posta è indicata dall'icona . Durante il

download degli aggiornamenti del database antivirus o dei moduli dell'applicazione, l'aspetto dell'icona passa a .

Se l'animazione dell'icona nell'area di notifica è disabilitata nelle impostazioni supplementari di Kaspersky Anti-Virus (vedere la sezione 5.10.4 a pagina 114), l'icona sarà disabilitata.

Se si verifica un importante evento antivirus, sopra l'icona viene visualizzato per qualche istante un messaggio informativo contenente una raccomandazione degli esperti di Kaspersky Lab (questa opzione non è disponibile in Windows98/NT).

3.2.2. Menu di scelta rapida

Facendo clic con il tasto destro del mouse sull'icona dell'applicazione nell'area di notifica (vedere la figura 1) viene visualizzato un menu di scelta rapida contenente le seguenti voci:

- **Apri Kaspersky Anti-Virus** apre la scheda **Protezione** della finestra principale del programma. Si ottiene lo stesso risultato facendo doppio clic sull'icona del programma nell'area di notifica.
- **Passa alla modalità utente/Passa alla modalità amministratore** - consente di passare dalla modalità utente alla modalità amministratore e viceversa.
- **Esecuzione delle attività in corso...** - si tratta di un elenco di attività lanciate secondo quanto pianificato. Questa voce viene visualizzata nel menu di scelta rapida durante l'esecuzione di una determinata attività.
- **Cerca virus nel computer** - lancia una scansione antivirus completa del computer in base al livello di protezione definito.
- **Aggiorna database antivirus** - lancia il processo di aggiornamento del database antivirus.
- **Attiva/Interrompi protezione in tempo reale** - abilita o disabilita la protezione in tempo reale del computer per un certo periodo. L'aspetto dell'icona cambierà in funzione dello stato della protezione in tempo reale (abilitata o disabilitata).

  Questa voce di menu è disponibile solo per gli amministratori di Kaspersky Anti-Virus. Gli utenti che non sono amministratori non possono abilitare né disabilitare la protezione in tempo reale del computer.

  Si sconsiglia di arrestare la protezione in tempo reale, poiché ciò aumenta notevolmente il rischio di infezione del computer con virus.

- **Informazioni** - visualizza una finestra di assistenza contenente informazioni su Kaspersky Anti-Virus 5.0 for Windows Workstations.
- **Esci** - chiude Kaspersky Anti-Virus. Solo l'amministratore di Kaspersky Anti-Virus può accedere a questa voce.

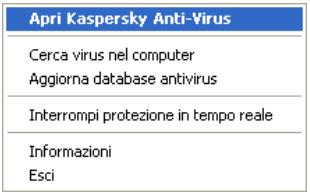

Figura 1. Menu di scelta rapida

3.2.3. La finestra principale dell'applicazione: struttura generale

La finestra principale di Kaspersky Anti-Virus consente di implementare tutte le funzioni del prodotto, per ottenere la massima protezione antivirus del computer. Questa finestra consente di:

- avviare ed arrestare la scansione completa del computer o di singole unità, cartelle o file, alla ricerca di virus e altri programmi pericolosi;
- creare attività di scansione degli oggetti definite dall'utente;
- scaricare gli aggiornamenti del database antivirus, del database degli attacchi di rete e dei moduli dell'applicazione:
- configurare le impostazioni della protezione antivirus;
- gestire gli oggetti in quarantena;
- gestire le copie degli oggetti create nella memoria di backup prima di disinfettarli od eliminarli;
- gestire i report;
- controllare la configurazione dell'applicazione, ecc.

Tutte le impostazioni della protezione antivirus, le informazioni necessarie e le attività sono raggruppate nelle seguenti schede della finestra principale:

- **Protezione** - stato ed attività della protezione antivirus (scansione degli oggetti e aggiornamento del database antivirus). Questa scheda consente di accedere alle funzioni che possono essere utilizzate per lavorare con la quarantena, la memoria di backup e i report. Questa è la scheda

principale da utilizzare per gestire l'applicazione (vedere la sezione 3.2.3.1 a pagina 27).

- **Impostazioni** - lo stato e le attività di definizione delle impostazioni principali della protezione antivirus (vedere la sezione 3.2.3.2 a pagina 29).
- **Assistenza** - visualizzazione delle informazioni relative alla chiave di licenza, rinnovo della licenza per l'applicazione, accesso alla guida dell'applicazione e invio di domande al Servizio di assistenza tecnica (vedere la sezione 3.2.3.3 a pagina 30).

Ciascuna scheda è suddivisa in due parti:

- *La parte sinistra della scheda* contiene collegamenti che consentono di accedere alle attività richieste durante l'utilizzo di Kaspersky Anti-Virus. L'elenco di attività dipende dall'obiettivo della scheda. Ad esempio, la scheda **Protezione** contiene le attività di scansione completa alla ricerca di virus, mentre la scheda **Impostazioni** consente di accedere alle attività di supporto della protezione antivirus.
- *La parte destra della scheda* contiene informazioni relative allo stato **corrente** della protezione antivirus (protezione in tempo reale, scansione completa del sistema e database antivirus). Quindi, la scheda **Protezione** indica lo stato della protezione antivirus, la scheda **Impostazioni** mostra lo stato delle sue impostazioni, mentre la scheda **Assistenza** visualizza lo stato della licenza (informazioni sulla chiave di licenza), i collegamenti alle informazioni per contattare l'assistenza e quelle sull'applicazione ed il sistema.

3.2.3.1. La scheda *Protezione*

La scheda **Protezione** (vedere la figura 2) è progettata per l'esecuzione delle attività che garantiscono la scansione completa del sistema come anche la scansione di singole unità, cartelle o singoli file. Questa finestra consente di:

- lanciare l'aggiornamento del database antivirus, dei moduli dell'applicazione e del database degli attacchi di rete;
- passare alla gestione dei report riguardanti l'esecuzione di tutte le attività lanciate (visualizzazione, eliminazione, esportazione ad un file);
- passare alla gestione degli oggetti in quarantena che possono essere infettati da virus o loro modifiche;
- passare alla gestione delle copie di backup di oggetti disinfettati o eliminati.

È possibile lanciare le attività tramite i relativi collegamenti.

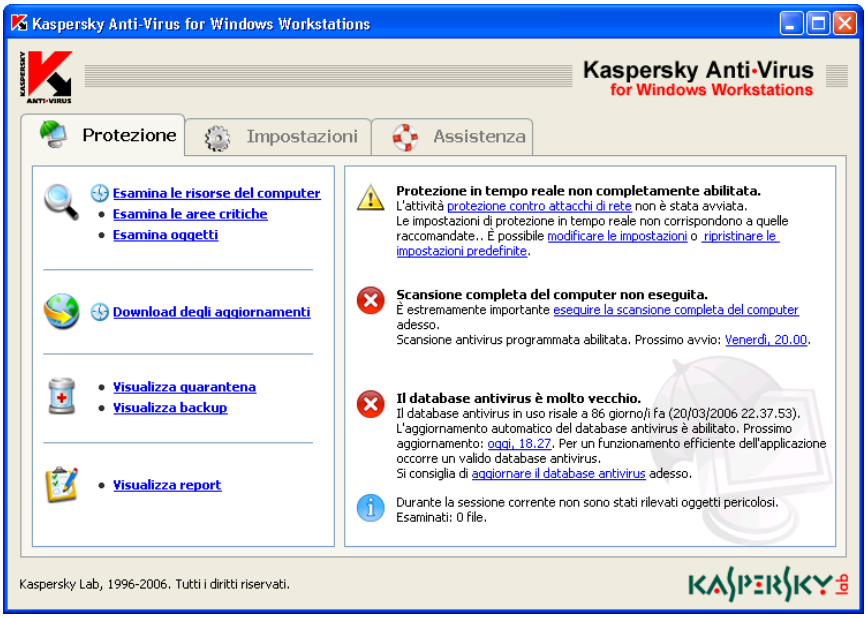
Kaspersky Anti-Virus for Windows Workstations
Kaspersky Anti-Virus
for Windows Workstations
Protezione
Impostazioni
Assistenza
Esamina le risorse del computer
Esamina le aree critiche
Esamina oggetti
Download degli aggiornamenti
Visualizza quarantena
Visualizza backup
Visualizza report
Protezione in tempo reale non completamente abilitata.
L'attività protezione contro attacchi di rete non è stata avviata.
Le impostazioni di protezione in tempo reale non corrispondono a quelle raccomandate.. È possibile modificare le impostazioni o ripristinare le impostazioni predefinite.
Scansione completa del computer non eseguita.
È estremamente importante eseguire la scansione completa del computer adesso.
Scansione antivirus programmata abilitata. Prossimo avvio: Venerdì, 20.00.
Il database antivirus è molto vecchio.
Il database antivirus in uso risale a 86 giorno/i fa (20/03/2006 22.37.53).
L'aggiornamento automatico del database antivirus è abilitato. Prossimo aggiornamento: oggi, 18.27. Per un funzionamento efficiente dell'applicazione occorre un valido database antivirus.
Si consiglia di aggiornare il database antivirus adesso.
Durante la sessione corrente non sono stati rilevati oggetti pericolosi.
Esaminati: 0 file.
Kaspersky Lab, 1996-2006. Tutti i diritti riservati.
KASPERSKY lab

Figura 2. La scheda **Protezione**

La parte destra della scheda visualizza *lo stato corrente della protezione in tempo reale, della scansione completa del computer e del database antivirus.* Ad esempio, la figura 2 mostra che la protezione in tempo reale è disabilitata e che è in corso una scansione completa del computer. Questa scheda contiene inoltre commenti relativi allo stato di ciascuna attività di protezione antivirus.

Gli stati critici e quelli non corrispondenti al livello di protezione raccomandato sono sempre accompagnati dalle *raccomandazioni degli esperti di Kaspersky Lab*. Per accrescere il livello di protezione antivirus, è possibile per esempio modificare le impostazioni correnti, ripristinare le impostazioni raccomandate dagli esperti, eseguire un'attività, ecc. Tutte le raccomandazioni vengono visualizzate come collegamenti che consentono di eseguire direttamente le azioni corrispondenti.

In caso di rilevamento di oggetti infetti o sospetti durante la scansione, le informazioni corrispondenti verranno visualizzate nella parte destra della scheda. Successivamente, è possibile passare all'elaborazione degli oggetti rilevati in qualsiasi momento seguendo il collegamento trattare questi oggetti (vedere la sezione 5.4 a pagina 87).

3.2.3.2. La scheda *Impostazioni*

La scheda **Impostazioni** (vedere la figura 3) contiene informazioni che consentono di valutare le impostazioni dell'applicazione e di modificare sia le impostazioni principali che quelle supplementari di Kaspersky Anti-Virus.

La parte destra della scheda visualizza le impostazioni correnti della protezione in tempo reale, della scansione manuale completa del computer e dell'aggiornamento del database antivirus, dei moduli dell'applicazione e del database degli attacchi di rete conosciuti, integrate da commenti dettagliati e suggerimenti per modificare alcune impostazioni. Ad esempio, se in passato il processo di aggiornamento del database antivirus è stato avviato manualmente, l'applicazione suggerisce di automatizzare tale processo pianificandone l'esecuzione automatica.

Seguendo i collegamenti visualizzati nella sezione sinistra della scheda è possibile passare alla modifica delle impostazioni di protezione in tempo reale, di scansione manuale e di aggiornamento. È inoltre possibile creare un elenco di oggetti da escludere dall'ambito della protezione e specificare il tipo di database antivirus da utilizzare.

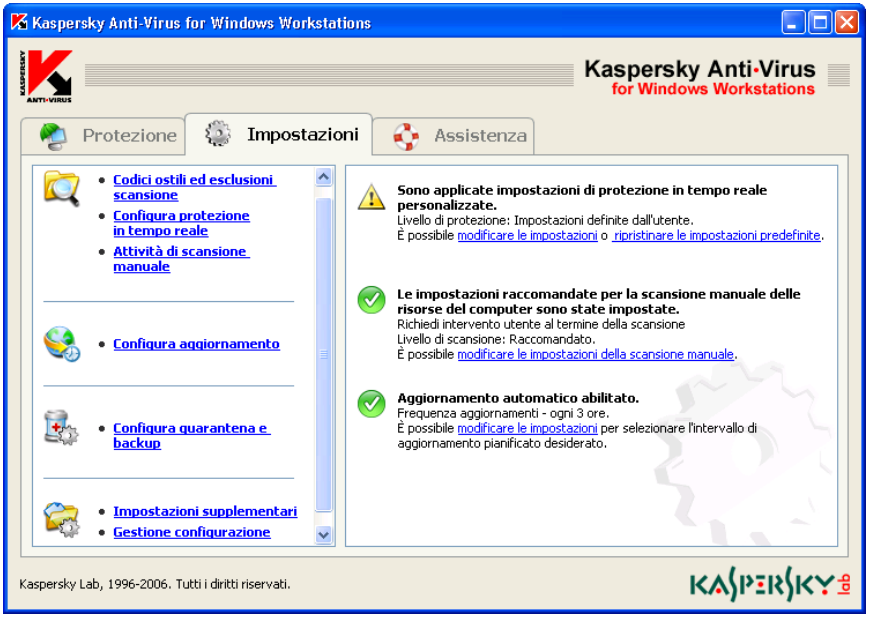
Kaspersky Anti-Virus for Windows Workstations
Kaspersky Anti-Virus
for Windows Workstations
Protezione
Impostazioni
Assistenza
Codici ostili ed esclusioni scansione
Configura protezione in tempo reale
Attività di scansione manuale
Configura aggiornamento
Configura quarantena e backup
Impostazioni supplementari
Gestione configurazione
Sono applicate impostazioni di protezione in tempo reale personalizzate.
Livello di protezione: Impostazioni definite dall'utente.
È possibile modificare le impostazioni o ripristinare le impostazioni predefinite.
Le impostazioni raccomandate per la scansione manuale delle risorse del computer sono state impostate.
Richiedi intervento utente al termine della scansione
Livello di scansione: Raccomandato.
È possibile modificare le impostazioni della scansione manuale.
Aggiornamento automatico abilitato.
Frequenza aggiornamenti - ogni 3 ore.
È possibile modificare le impostazioni per selezionare l'intervallo di aggiornamento pianificato desiderato.
Kaspersky Lab, 1996-2006. Tutti i diritti riservati.
KASPERSKY lab

Figura 3. La scheda **Impostazioni**

Questa scheda consente inoltre di configurare le impostazioni della quarantena, utilizzata per archiviare i file potenzialmente infettati da virus o loro modifiche, e della memoria di backup, utilizzata per archiviare le copie di backup degli oggetti. È possibile passare alla configurazione delle impostazioni supplementari di Kaspersky Anti-Virus seguendo il collegamento Impostazioni supplementari.

Kaspersky Anti-Virus consente di creare diverse configurazioni da utilizzare per il suo funzionamento, salvandole in file speciali detti *profili*. Successivamente, è possibile tornare alla configurazione desiderata. Per fare ciò, non sarà necessario riconfigurare l'applicazione: sarà sufficiente caricare il profilo desiderato. Per passare alla creazione ed al caricamento dei profili, seguire il collegamento Gestione configurazione.

3.2.3.3. La scheda *Assistenza*

La scheda **Assistenza** (vedere la figura 4) visualizza informazioni su come contattare l'assistenza in caso di problemi nell'utilizzo di Kaspersky Anti-Virus o in situazioni non gestibili autonomamente. Questa scheda contiene inoltre informazioni sull'applicazione, la chiave di licenza ed il sistema operativo installato sul computer, quando è necessario fornire queste informazioni al Servizio di assistenza tecnica di Kaspersky Lab. Queste informazioni sono visualizzate nella sezione destra della scheda.

I collegamenti nella parte sinistra consentono di:

- inviare al Servizio di assistenza tecnica di Kaspersky Lab richieste ed oggetti potenzialmente infetti da virus e loro modifiche per l'analisi.
- rinnovare la licenza per Kaspersky Anti-Virus.

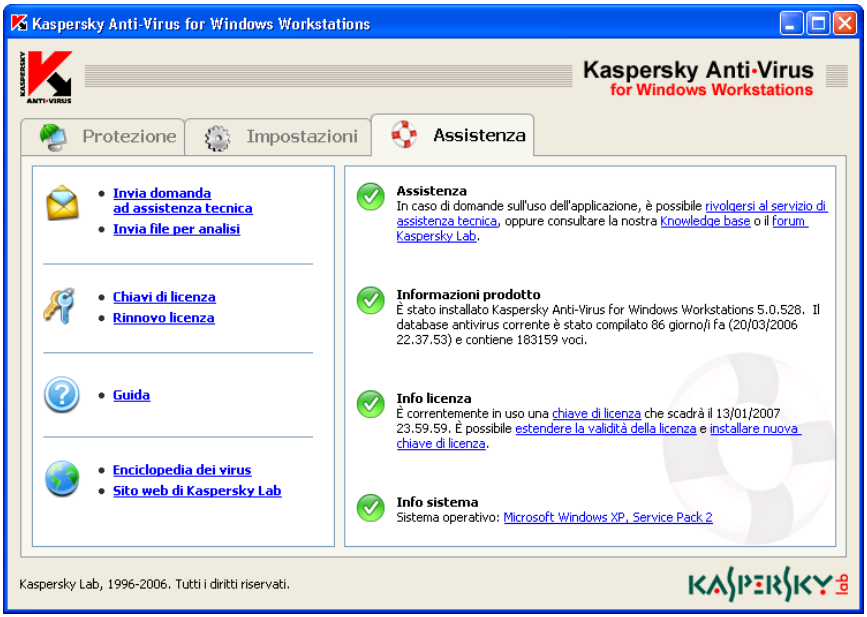
Kaspersky Anti-Virus for Windows Workstations
Kaspersky Anti-Virus
for Windows Workstations
Protezione
Impostazioni
Assistenza
Invia domanda ad assistenza tecnica
Invia file per analisi
Chiavi di licenza
Rinnovo licenza
Guida
Enciclopedia dei virus
Sito web di Kaspersky Lab
Assistenza
In caso di domande sull'uso dell'applicazione, è possibile rivolgersi al servizio di assistenza tecnica, oppure consultare la nostra Knowledge base o il forum Kaspersky Lab.
Informazioni prodotto
È stato installato Kaspersky Anti-Virus for Windows Workstations 5.0.528. Il database antivirus corrente è stato compilato 86 giorno/i fa (20/03/2006 22.37.53) e contiene 183159 voci.
Info licenza
È correntemente in uso una chiave di licenza che scadrà il 13/01/2007 23.59.59. È possibile estendere la validità della licenza e installare nuova chiave di licenza.
Info sistema
Sistema operativo: Microsoft Windows XP, Service Pack 2
Kaspersky Lab, 1996-2006. Tutti i diritti riservati.
KASPERSKY lab

Figura 4. La scheda **Assistenza**

La sezione sinistra della scheda contiene inoltre collegamenti alle informazioni della guida:

- Guida - guida dell'applicazione.
- Enciclopedia dei virus - collegamento al sito Web www.viruslist.com contenente descrizioni dettagliate di tutti i programmi pericolosi attualmente esistenti.
- Sito Web di Kaspersky Lab - collegamento al sito Web di Kaspersky Lab.

3.2.4. La finestra Scansione in corso

La finestra del processo di scansione viene visualizzata quando viene lanciata una scansione del computer o dei suoi oggetti singoli (dischi, cartelle, file) (vedere la Figura 5).

Essa comprende due sezioni:

- La sezione superiore della finestra contiene un indicatore che mostra il progresso percentuale dell'attività di scansione, il nome dell'oggetto esaminato, una stima del tempo rimanente ed i dati statistici generali, tra

cui il numero di oggetti esaminati fino ad ora ed il numero di oggetti che sono stati disinfettati, eliminati e messi in quarantena

- La sezione inferiore della finestra si apre scegliendo il pulsante e contiene tre schede: **Report**, contenente il rapporto sugli eventi verificatisi durante la scansione, **Statistiche**, contenente i risultati della scansione, e **Impostazioni**, contenente l'elenco di impostazioni utilizzate per eseguire la scansione. Per nascondere la sezione inferiore, utilizzare il pulsante .

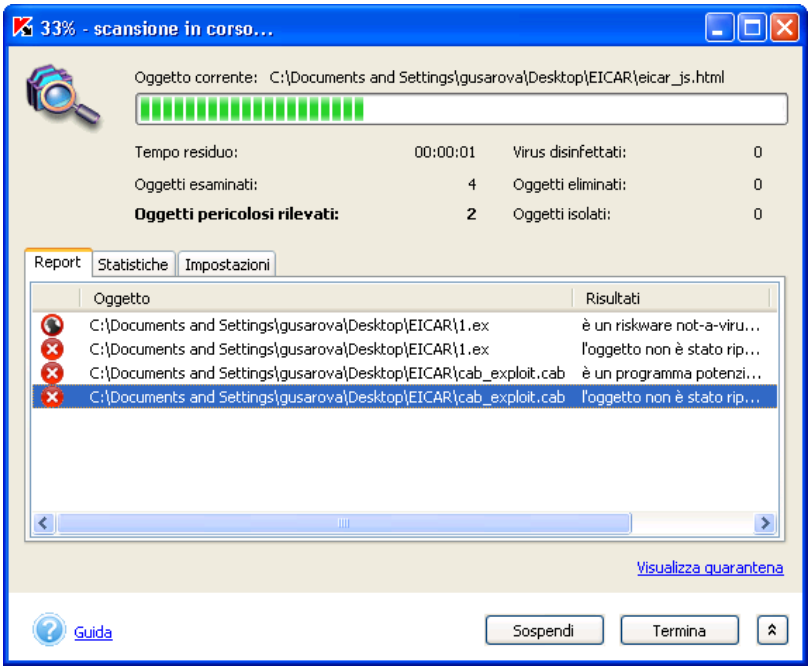

Figura 5. Finestra di scansione

Per accedere alla finestra della quarantena (vedere la sezione 5.10.1.2 a pagina 105), seguire il collegamento Visualizza quarantena.

Se è in corso una scansione completa del computer, la stessa finestra consente di selezionare una modalità che spegne il computer una volta terminata la scansione. Ciò è utile se, ad esempio, si avvia la scansione del computer al termine della giornata lavorativa e non si desidera attenderne il completamento.

Tuttavia, l'utilizzo di questa modalità richiede le seguenti preparazioni: prima di avviare la scansione, è necessario disabilitare la richiesta della password

durante la scansione degli oggetti (vedere la sezione 5.3.3.1 a pagina 79), se essa è abilitata, ed impostare l'elaborazione automatica degli oggetti pericolosi, la loro eliminazione o messa in quarantena, oppure la registrazione delle informazioni nel report (vedere la sezione 5.3.3.2 a pagina 82). Il risultato di queste azioni sarà la disabilitazione della modalità interattiva di funzionamento dell'applicazione e la scansione non verrà interrotta (vale a dire, non verranno visualizzate richieste).

Per spegnere il computer al termine della scansione, selezionare la casella **Spegni il computer al termine della scansione** nella finestra di scansione.

3.2.5. La guida

Informazioni complete sul programma sono disponibili dalla scheda **Assistenza** della finestra principale dell'applicazione: basta seguire il collegamento Guida nella parte sinistra della scheda.

In caso di domande su una finestra di dialogo specifica, premere il tasto **<F1>** oppure fare clic su Guida nell'angolo inferiore sinistro della finestra di dialogo stessa.

CAPITOLO 4. PROTEZIONE DEL COMPUTER UTILIZZANDO LE IMPOSTAZIONI PREDEFINITE

La protezione antivirus è attiva subito dopo l'installazione dell'applicazione, con le impostazioni predefinite. Tali impostazioni sono quelle raccomandate dagli esperti di Kaspersky Lab per una protezione ottimale del computer.

Se si utilizza la funzione di amministrazione centralizzata tramite Kaspersky Administration Kit, le impostazioni possono essere determinate dalle regole e dalle attività create dall'amministratore della sicurezza. Ciò richiede l'attivazione di un "blocco" sulle corrispondenti impostazioni. Per maggiori dettagli, vedere la guida di Kaspersky Administration Kit 5.0.

Inoltre, esiste la possibilità di modificare le impostazioni con facilità selezionando uno dei tre livelli di protezione predefiniti dagli esperti di Kaspersky Lab: *protezione massima, raccomandato e alta velocità.*

4.1. Impostazioni predefinite

Le seguenti impostazioni predefinite vengono specificate per ciascuna attività di protezione antivirus:

PROTEZIONE IN TEMPO REALE IN MODALITÀ DI MONITORAGGIO

Il livello *raccomandato* di protezione con le seguenti impostazioni è l'impostazione predefinita della protezione in tempo reale:

- L'applicazione controlla i file aperti per lettura, scrittura ed esecuzione, in particolare:
  - file su dischi fissi, unità rimovibili e settori di boot;
  - file su unità di rete;
  - file compressi, oggetti OLE e flussi NTFS supplementari.
- Le tecnologie iChecker™ e iStreams™ sono abilitate;

- In caso di rilevamento di oggetti infetti, Kaspersky Anti-Virus cerca di disinfettarli; se la disinfezione non riesce li elimina dopo averne creato una copia nella memoria di backup; gli oggetti sospetti vengono messi in quarantena.
- Se vengono rilevati programmi potenzialmente pericolosi, Kaspersky Anti-virus ne blocca l'esecuzione, aggiungendo le informazioni su tali programmi al report.
- L'applicazione esamina i messaggi di posta elettronica:
    - La scansione dei messaggi in arrivo inviati tramite il protocollo POP3 è abilitata; i file contenuti negli archivi vengono esaminati.
    - La scansione dei messaggi in uscita inviati tramite il protocollo SMTP è disabilitata.
- L'applicazione esamina le macro scritte in VBA usate dalla suite Microsoft Office; in caso di rilevamento di uno script sospetto, Kaspersky Anti-Virus ne blocca l'esecuzione.
- L'applicazione esamina gli script dinamici VBScript e JavaScript elaborati da Microsoft Internet Explorer o dal motore di elaborazione degli script di Windows. In caso di rilevamento di script sospetti, Kaspersky Anti-Virus ne blocca l'esecuzione.
- La protezione contro gli attacchi di rete è disabilitata.

SCANSIONE ANTIVIRUS MANUALE

Il livello *raccomandato* di protezione con le seguenti impostazioni è quello predefinito per la scansione completa del sistema:

- la scansione completa è pianificata per l'esecuzione ogni venerdì alle 20:00;
- l'ambito di scansione comprende:
    - tutti i file sui dischi rigidi e i settori di boot;
    - i file nella RAM, gli oggetti lanciati automaticamente durante il caricamento del sistema operativo (oggetti d'avvio) e i flussi NTFS supplementari.
    - i file compressi, gli archivi, gli archivi autoestraenti e gli oggetti OLE.

La scansione completa del computer non comprende le caselle di posta.

- Le tecnologie iChecker™ e iStreams™ sono abilitate;

- gli oggetti sulle unità di rete, i database di posta elettronica e i file in formato testo di posta elettronica non saranno esaminati.
- Kaspersky Anti-Virus rimanda l'elaborazione degli oggetti infetti o sospetti eventualmente rilevati durante la scansione al termine della stessa, richiedendo all'utente l'azione da eseguire per elaborarli.
- Se vengono rilevati programmi potenzialmente pericolosi (riskware), Kaspersky Anti-virus li ignora, aggiungendo le informazioni su tali programmi al report.

AGGIORNAMENTO DEI DATABASE ANTIVIRUS E DEI MODULI DELL'APPLICAZIONE

Le impostazioni predefinite per l'aggiornamento dei database antivirus e dei moduli dell'applicazione sono le seguenti:

- l'esecuzione della procedura di aggiornamento è pianificata ogni tre ore a partire dall'installazione di Kaspersky Anti-Virus;

Se il computer lavora meno di 3 ore al giorno, il database sarà aggiornato immediatamente al prossimo avvio di Kaspersky Anti-Virus.

- l'aggiornamento dei database antivirus e gli aggiornamenti critici di Kaspersky Anti-Virus sono abilitati. Verrà visualizzata una richiesta di conferma prima di installare gli aggiornamenti.

MESSA IN QUARANTENA DEGLI OGGETTI SOSPETTI

Le impostazioni predefinite per la quarantena sono le seguenti:

- lo spazio riservato agli oggetti in quarantena non è soggetto a restrizioni;
- gli oggetti vengono conservati in quarantena per 90 giorni.

SALVATAGGIO DELLA COPIA DI UN OGGETTO INFETTO

Prima di cercare di disinfettare o eliminare un oggetto, il programma salva una copia di ciascun oggetto infetto nella memoria di backup. Le impostazioni predefinite sono le seguenti:

- lo spazio riservato alla memoria di backup non è soggetto a restrizioni;
- gli oggetti di backup vengono conservati per 90 giorni.

4.2. Livelli di protezione antivirus

Per consentire una facile modifica delle impostazioni di protezione antivirus, l'applicazione propone tre livelli con impostazioni predefinite (vedere la Tabella1).

- **Protezione massima** - il livello massimo di protezione antivirus del computer, che comporta un certo rallentamento del sistema.
- **Raccomandato** - livello di protezione antivirus basato sulle impostazioni raccomandate dagli esperti di Kaspersky Lab, che consente una protezione ottimale del computer.
- **Alta velocità** - livello di protezione antivirus che garantisce le massime prestazioni del sistema grazie alla riduzione del numero di oggetti esaminati.

Se le impostazioni di uno qualsiasi di questi livelli vengono modificate tramite l'interfaccia locale o la consolle di amministrazione di Kaspersky Administration Kit 5.0, la descrizione del livello passerà alla dicitura **Impostazioni definite dall'utente**. Questo è il quarto livello di protezione antivirus, con impostazioni definite dall'utente.

Se le impostazioni sono state modificate tramite la consolle di amministrazione, la parte destra della scheda **Protezione** indicherà che le impostazioni sono state configurata dall'amministratore.

La seguente tabella mostra i valori delle impostazioni per i livelli predefiniti di protezione in tempo reale (**protezione**) e della scansione manuale (**scansione**).

Legenda:

+ abilitato;

– disabilitato;

x non disponibile per questa attività.

Tabella1. Configurazione delle impostazioni del livello di protezione

Impostazione	Protezione massima		Raccomandato		Alta velocità	
	protezione	scansione	protezione	scansione	protezione	scansione
usa IChecker	+	+	+	+	+	+
usa IStreams	+	+	+	+	+	+
livello di scansione	file di formato specifico	tutti i file	file di formato specifico	tutti i file	file con estensione specifica	file di formato specifico
dimensione dell'oggetto esaminato, non più di (MB)	x	–	x	–	x	8
durata della scansione, non più di (sec.)	60	–	60	–	60	60

Impostazione	Protezione massima		Raccomandato		Alta velocità	
	protezione	scansione	protezione	scansione	protezione	scansione
dischi rigidi	+	x	+	x	+	x
unità rimovibili	+	x	+	x	+	x
unità di rete	+	x	+	x	–	x
flussi NTFS	+	+	+	+	+	+
settori di boot del disco	+	+	+	+	+	+
file compressi	+	+	+	+	+	+
archivi	x	+	x	+	x	–
archivi autoestraenti	+	+	–	+	–	+
database di posta	x	+	x	–	x	–
file in formato testo di posta elettronica	x	+	x	–	x	–
oggetti OLE	+	+	+	+	–	+

CAPITOLO 5. GESTIONE DELL'APPLICAZIONE TRAMITE L'INTERFACCIA LOCALE

Questo capitolo contiene informazioni dettagliate sul funzionamento e le impostazioni delle attività principali di Kaspersky Anti-Virus, nonché sulle funzioni supplementari di controllo del programma tramite l'interfaccia locale.

5.1. Aggiornamento del database antivirus e dei moduli dell'applicazione

Kaspersky Anti-Virus consente di automatizzare l'aggiornamento sia del database antivirus, contenente la descrizione dei singoli virus e delle procedure per la loro eliminazione, sia dei moduli dell'applicazione, il tutto attraverso gli appositi server di Kaspersky Lab.

Gli aggiornamenti del database antivirus sono essenziali per la protezione del computer. Tutti i giorni vengono creati molti nuovi virus, e gli esperti di Kaspersky Lab inseriscono quotidianamente informazioni su tali virus nel database antivirus. Si consiglia di aggiornare il database antivirus almeno una volta ogni tre ore, e il più spesso possibile durante le epidemie più gravi; l'ideale sarebbe ogni ora.

Durante il download degli aggiornamenti, Kaspersky Anti-Virus si collega al server degli aggiornamenti http o ftp di Kaspersky Lab specificato dall'utente, oppure ad una cartella locale o di rete sul computer. Se si utilizza Kaspersky Administration Kit per gestire l'applicazione, gli aggiornamenti possono essere eseguiti dalla cartella degli aggiornamenti ubicata sul *server di amministrazione*.

È possibile lanciare manualmente il programma di aggiornamento oppure pianificarne l'avvio. Per ottenere le versioni aggiornate del database antivirus al momento giusto, si consiglia di pianificare l'avvio automatico di tale procedura (per maggiori dettagli sulla pianificazione, vedere la sezione 5.8 a pagina 98).

5.1.1. Quando scaricare gli aggiornamenti

L'applicazione notifica quando il database antivirus deve essere aggiornato. È anche possibile giudicare autonomamente la necessità di eseguire l'aggiornamento in base allo stato indicato nella sezione destra della scheda **Protezione** (vedere la figura 2).

Lo stato degli aggiornamenti è indicato da una delle seguenti icone:

il database antivirus è stato aggiornato recentemente, oppure l'aggiornamento è in corso

è necessario aggiornare il database antivirus. Se l'aggiornamento è impossibile perché la chiave di licenza è scaduta, l'applicazione proporrà la consultazione delle informazioni relative al rinnovo della licenza.

l'aggiornamento è urgente poiché il database antivirus è totalmente obsoleto, mancante o corrotto.

5.1.2. Aggiornamento manuale. Download degli aggiornamenti

Per lanciare manualmente il processo di aggiornamento,

utilizzare il collegamento Download degli aggiornamenti nella sezione sinistra della scheda **Protezione**,

oppure:

il collegamento aggiornare il database antivirus nella notifica sullo stato del database antivirus, nella sezione destra della scheda **Protezione**;

oppure:

selezionare la voce **Aggiorna database antivirus** dal menu di scelta rapida che si apre facendo clic con il tasto destro del mouse sull'icona dell'applicazione nell'area di notifica.

Facendo ciò si apre una finestra (vedere la figura 6) contenente informazioni sul progresso dell'aggiornamento del database antivirus e dei moduli dell'applicazione.

La procedura di download degli aggiornamenti può essere suddivisa nei seguenti passaggi:

1. Kaspersky Anti-Virus verifica la connessione alla rete e stabilisce il collegamento con la sorgente degli aggiornamenti.
2. L'applicazione ottiene dai server di aggiornamento di Kaspersky Lab un elenco degli aggiornamenti disponibili ed informazioni sulle loro dimensioni.
3. Il programma confronta lo stato del database antivirus e dei moduli del applicazione sul computer con lo stato di quelli ubicati presso l'origine degli aggiornamenti. Se il computer è dotato della più recente versione del database antivirus, il processo di aggiornamento termina qui. In caso contrario, i file vengono copiati sul computer.

   L'avanzamento del download viene visualizzato tramite l'indicatore del processo di copia. La dimensione degli aggiornamenti ricevuti è indicata nel campo **Aggiornamenti scaricati**.
4. Il programma connette automaticamente il database antivirus scaricato. Se l'operazione riesce, Kaspersky Anti-Virus inizia ad utilizzare il database per eseguire la scansione del computer. Se la connessione del nuovo database antivirus non riesce, verrà ripristinata automaticamente la versione precedente del database.

Per garantire una corretta connessione degli aggiornamenti ricevuti, potrebbe essere necessario riavviare il computer. In tal caso verrà visualizzata una notifica corrispondente.

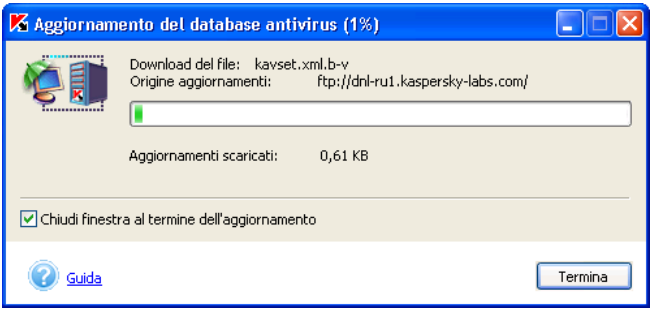

Figura 6. Aggiornamento del database antivirus e dei moduli dell'applicazione

5.1.3. Configurazione degli aggiornamenti

Per configurare le impostazioni dell'attività di aggiornamento del database antivirus:

utilizzare il collegamento Configura aggiornamento nella sezione sinistra della scheda **Impostazioni** (vedere la figura 3).

Ciò aprirà la finestra **Aggiornamento del database antivirus** (vedere la Figura 7).

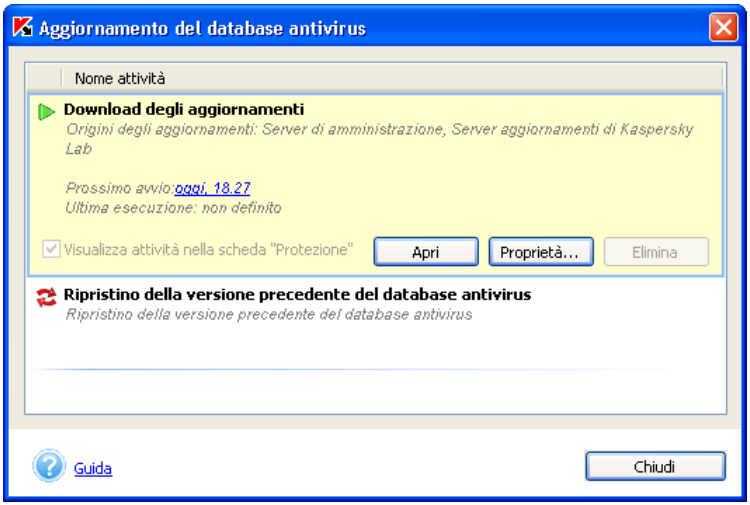

Figura 7. Elenco delle attività di aggiornamento del database antivirus

Il blocco contenente informazioni sull'origine di aggiornamento e l'ora di avvio dell'ultimo e del prossimo aggiornamento si apre facendo clic sul nome dell'attività. Questo blocco consente di lanciare manualmente l'aggiornamento del database antivirus utilizzando il pulsante **Esegui**, o di aprire la finestra di configurazione delle impostazioni di aggiornamento del database antivirus utilizzando il pulsante **Proprietà...** (vedere la Figura 8), che consente di:

- pianificare il lancio automatico del processo di aggiornamento (vedere la sezione 5.8 a pagina 98);
- abilitare la funzione di aggiornamento dei moduli dell'applicazione di Kaspersky Anti-Virus (vedere la sezione 5.1.3.1 a pagina 44);

- configurare la funzione di copia degli aggiornamenti in una cartella locale per poi trasmetterli agli altri computer della rete sui quali è installato Kaspersky Anti-Virus (vedere la sezione 5.1.3.2 a pagina 46).
- selezionare l'origine degli aggiornamenti; i server degli aggiornamenti http o ftp di Kaspersky Lab, indicati dall'utente, o una cartella locale o di rete (vedere la sezione 5.1.3.3 a pagina 47);
- configurare le impostazioni del server proxy (vedere la sezione 5.1.3.4 a pagina 49);
- configurare l'avvio dell'attività tramite un diverso account utente (solo per computer che eseguono Microsoft Windows NT/2K/XP) (vedere la sezione 5.9 a pagina 101);
- selezionare il tipo di database antivirus da scaricare (vedere la sezione 5.1.3.5 a pagina 50).

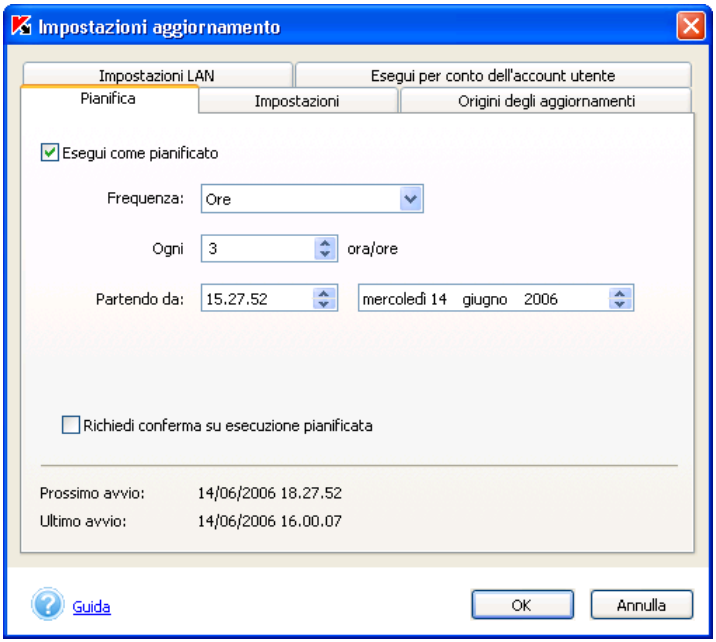

Figura 8. Configurazione delle impostazioni dell'attività di aggiornamento del database antivirus

Il **Ripristino della versione precedente del database antivirus** non prevede impostazioni. Questa attività può solo essere lanciata per ripristinare la versione precedente del database antivirus.

5.1.3.1. Aggiornamento dei moduli dell'applicazione

Oltre al database antivirus, è possibile anche aggiornare i moduli dell'applicazione di Kaspersky Anti-Virus. I file di aggiornamento dei moduli dell'applicazione vengono caricati sui server di aggiornamento alla pubblicazione.

È possibile aggiornare i moduli dell'applicazione dall'origine degli aggiornamenti specificata durante l'impostazione dell'applicazione (vedere la sezione 5.1.3.3 a pagina 47). Per fare ciò, è sufficiente selezionare la casella **Installa gli aggiornamenti ai moduli applicazione** nella scheda **Impostazioni** della finestra **Impostazioni aggiornamento** (vedere la Figura 9). Selezionare quali aggiornamenti si desidera installare:

- **Solo aggiornamenti critici**
- **Tutti gli aggiornamenti disponibili**

Se si desidera che gli aggiornamenti ai moduli dell'applicazione siano installati automaticamente una volta scaricati, deselezionare la casella **Richiedi conferma prima di installare**.

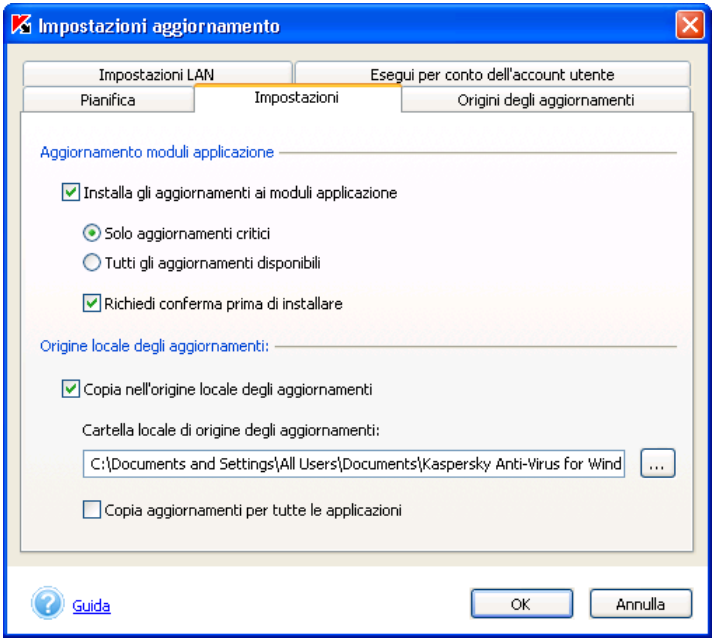

Figura 9. Finestra di configurazione delle impostazioni di aggiornamento. La scheda **Impostazioni**

Se si ordina un archivio zip con gli aggiornamenti presso Kaspersky Lab o uno dei suoi partner, specificare se si desidera ricevere anche gli aggiornamenti ai moduli dell'applicazione.

Quando si ricevono i moduli dell'applicazione, sullo schermo verrà visualizzata una corrispondente richiesta di conferma (vedere la Figura 10). Selezionare una delle seguenti opzioni:

- **Installa gli aggiornamenti ai moduli applicazione**.
- **Non installare gli aggiornamenti ai moduli applicazione, visualizza in seguito** - ricorda l'installazione degli aggiornamenti ai moduli dell'applicazione al prossimo avvio di Kaspersky Anti-Virus.
- **Disabilita l'installazione degli aggiornamenti ai moduli applicazione** - se si seleziona questa opzione, la casella **Installa gli aggiornamenti ai moduli applicazione** nella scheda **Impostazioni** della finestra **Impostazioni aggiornamento** (vedere la Figura 9) sarà deselezionata, e la funzione di aggiornamento dei moduli dell'applicazione sarà disabilitata.

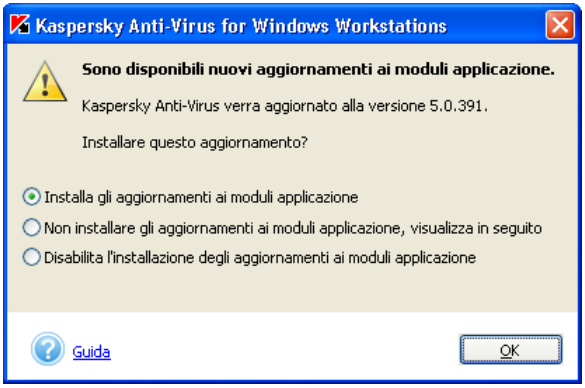
Kaspersky Anti-Virus for Windows Workstations
Sono disponibili nuovi aggiornamenti ai moduli applicazione.
Kaspersky Anti-Virus verra aggiornato alla versione 5.0.391.
Installare questo aggiornamento?
Installa gli aggiornamenti ai moduli applicazione
Non installare gli aggiornamenti ai moduli applicazione, visualizza in seguito
Disabilita l'installazione degli aggiornamenti ai moduli applicazione
Guida
OK

Figura 10. Richiesta di conferma per l'installazione dei moduli dell'applicazione

5.1.3.2. Copia degli aggiornamenti nella cartella locale

È possibile configurare il funzionamento del servizio di copia degli aggiornamenti nella scheda **Impostazioni** (vedere la Figura 9). Questo servizio consente di salvare gli aggiornamenti al database antivirus e ai moduli dell'applicazione scaricati dai server di aggiornamento di Kaspersky Lab in una cartella locale, alla quale gli altri computer (sui quali sia installato Kaspersky Anti-Virus) potranno accedere per prelevarli, riducendo il traffico Internet.

Per abilitare il servizio di copia degli aggiornamenti, selezionare la casella **Copia nell'origine locale degli aggiornamenti** . Specificare il percorso alla cartella nel campo di testo **Cartella locale di origine degli aggiornamenti**.

Inoltre, è possibile selezionare il metodo per copiare gli aggiornamenti:

- *completo* - prevede la copia degli aggiornamenti al database antivirus e ai moduli di tutte le applicazioni di Kaspersky Lab. Per selezionare l'aggiornamento completo, selezionare la casella **Copia aggiornamenti per tutte le applicazioni**.
- *selettivo* - prevede la copia degli aggiornamenti al database antivirus e ai moduli dell'applicazione solo per Kaspersky Anti-Virus 5.0 for Windows Workstations e Kaspersky Anti-Virus 5.0 for Windows File Servers. Per selezionare questo metodo d'aggiornamento, la casella **Copia aggiornamenti per tutte le applicazioni** deve essere deselezionata (essa è selezionata per impostazione predefinita).

5.1.3.3. Selezione dell'origine degli aggiornamenti

È possibile selezionare l'origine degli aggiornamenti nella scheda **Origini degli aggiornamenti** della finestra **Impostazioni aggiornamento** (vedere la Figura 11).

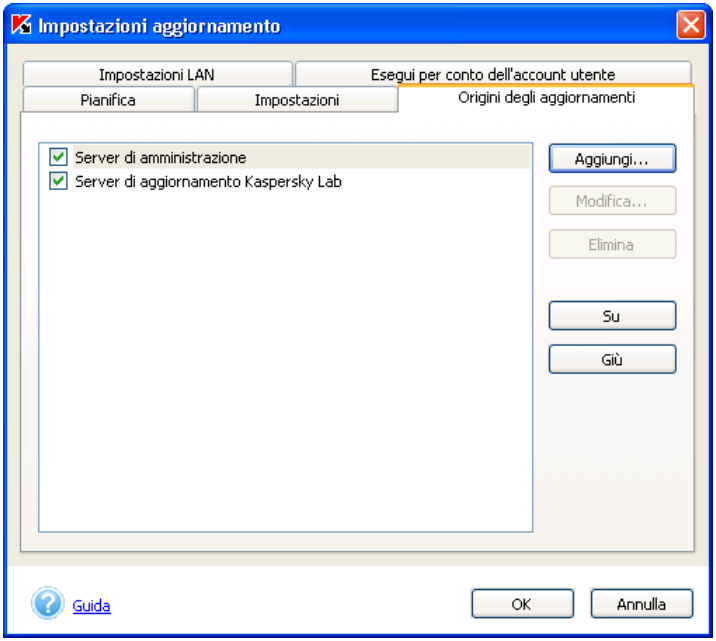

Figura 11. Finestra Impostazioni aggiornamento.
La scheda **Origini degli aggiornamenti**.

È possibile specificare le seguenti origini degli aggiornamenti:

- *Server di amministrazione* - si tratta di una memoria centralizzata per gli aggiornamenti, ubicata presso il Server di amministrazione di Kaspersky Administration Kit. Questa origine degli aggiornamenti non sarà disponibile se l'agente di rete non è installato sul computer (per dettagli, vedere la guida di Kaspersky Administration Kit 5.0).
- *Server di aggiornamento Kaspersky Lab* - sono i siti Internet di Kaspersky Lab sui quali vengono caricati il database antivirus e i moduli dell'applicazione aggiornati.
- I *server ftp o http* contenenti nuovi aggiornamenti, aggiunti dall'utente.

- *una cartella di rete o locale.*

Per impostazione predefinita, gli aggiornamenti vengono scaricati dai servizi di aggiornamento Internet di Kaspersky Lab, oppure dal Server di amministrazione se si utilizza Kaspersky Administration Kit 5.0. Questo elenco può essere ampliato con ulteriori origini degli aggiornamenti. Per fare ciò, scegliere il pulsante **Aggiungi...** , quindi selezionare il tipo di origine - *Server o Cartella*. Se è stato selezionato il tipo di origine *Server*, immettere l'indirizzo del server ftp o http nella finestra che verrà aperta (quando si specifica il nome del server sarà necessario inserire il prefisso del protocollo che si desidera utilizzare, ad esempio, *http://server.net* o *ftp://10.0.0.1*). Se è stato selezionato il tipo di origine *Cartella*, specificare il percorso alla cartella che contiene gli aggiornamenti.

È possibile cambiare le impostazioni per l'origine degli aggiornamenti tramite il pulsante **Modifica...**. È possibile modificare l'indirizzo per il tipo di origine *Server* oppure modificare il percorso per il tipo di origine *Cartella*.

È possibile selezionare la regione del server di Kaspersky Lab dal quale saranno copiati gli aggiornamenti selezionando il paese corrispondente dall'elenco a discesa **Percorso** (vedere la Figura 12). Per impostazione predefinita, verrà selezionato il paese corrispondente alle impostazioni regionali del sistema operativo. Si raccomanda di specificare la posizione corrente, in modo da scegliere il server più vicino. Ciò accelererà il download degli aggiornamenti e ne abbrevierà la durata. È inoltre possibile disabilitare l'utilizzo del server proxy selezionando la casella corrispondente.

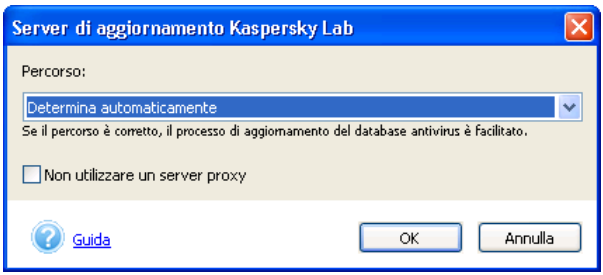

Figura 12. Modifica delle impostazioni per l'origine degli aggiornamenti. Selezionare la regione geografica di ubicazione del server.

Se si desidera eseguire l'aggiornamento dall'origine specificata, selezionare la casella accanto all'origine stessa. È possibile selezionare diverse origini contemporaneamente. In tal caso, Kaspersky Anti-Virus eseguirà gli aggiornamenti dalla prima origine nell'elenco. Se per qualsiasi ragione questa origine non è disponibile, l'aggiornamento verrà eseguito dall'origine successiva nell'elenco, e così via. È possibile modificare l'ordine delle origini nell'elenco utilizzando i pulsanti **Su** e **Giù**.

Se non è possibile accedere ai server di aggiornamento di Kaspersky Lab (ad esempio, perché non si dispone di accesso a Internet), rivolgersi al nostro ufficio centrale [+7 (495) 797-87-00] per informarsi sull'ubicazione dei partner di Kaspersky Lab, che potranno fornire il database antivirus su floppy disk o CD, in formato zip.

Quando si ordina il database antivirus, specificare il tipo di database (standard o esteso) che si desidera ricevere (vedere la sezione 5.1.3.5 a pagina 50).

Decomprimere l'archivio zip contenente il database antivirus in qualsiasi cartella del computer, e impostare questa cartella come origine degli aggiornamenti.

5.1.3.4. Configurazione delle impostazioni del server proxy

Le impostazioni relative alla connessione di rete possono essere configurate nella scheda **Impostazioni LAN** (vedere la Figura 13). Ci sono due opzioni disponibili per determinare le impostazioni del server proxy:

- **Rileva automaticamente l'impostazione del server proxy**
- **Usa un server proxy diverso**

La prima opzione è quella predefinita; in questo caso le impostazioni verranno copiate da Microsoft Internet Explorer. Se il server proxy richiedere l'autorizzazione, selezionare la seconda opzione e specificare manualmente l'impostazione del server proxy:

Indirizzo - l'indirizzo IP del server proxy in formato decimale (ad esempio, 10.10.10.102*),* oppure il suo nome.

Porta - il numero di porta sul quale è installato il server proxy. Selezionare uno dei valori suggeriti: *3128*, *8080*, *8082*, *8903* dall'elenco a discesa, oppure immettere il valore desiderato.

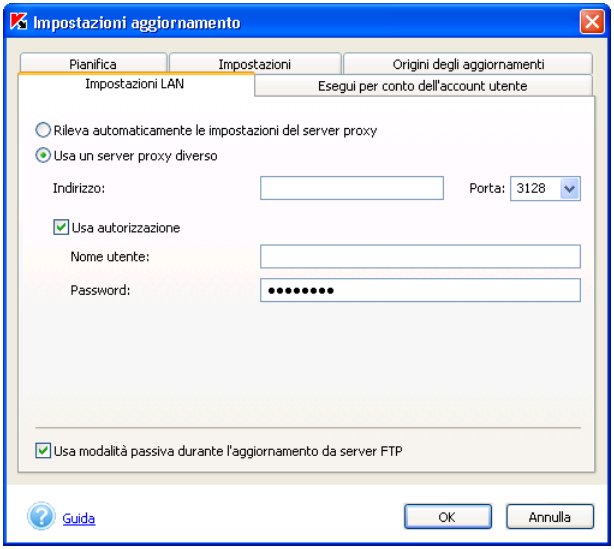

Figura 13. Configurazione delle impostazioni LAN

Se il server proxy richiedere l'autorizzazione, selezionare la casella **Usa autorizzazione** ed immettere il nome utente e la password nei campi sottostanti.

Se è richiesta l'autorizzazione per il server proxy e non sono stati immessi il nome utente e la password, oppure i valori immessi non sono stati accettati dal server proxy, quando si avvia il processo di aggiornamento si aprirà una finestra richiedente il nome utente e la password ai fini di autorizzazione. Se l'autorizzazione riesce, il nome utente e la password specificati verranno utilizzati per il prossimo aggiornamento. In caso contrario, i parametri di autorizzazione verranno richiesti nuovamente.

Se il server ha un firewall e non si riesce a collegarsi al server FTP richiesto in modalità attiva, selezionare la casella **Usa modalità passiva durante l'aggiornamento da server FTP**.

5.1.3.5. Selezione del tipo di database antivirus

Kaspersky Anti-Virus consente di scegliere tra due tipi di database antivirus che possono essere utilizzati dall'applicazione:

- *Database standard* - è il database antivirus che contiene le voci relative a tutti i programmi dannosi conosciuti fino ad ora ed ai metodi utilizzati per trattarli.

- Se si desidera proteggere i dati memorizzati sul computer dai programmi potenzialmente pericolosi, è necessario utilizzare il *Database antivirus esteso*. Oltre alle voci contenute nel database standard, questo database contiene descrizioni di adware, spyware, strumenti di hacking e altri riskware.

L'utilizzo del database antivirus standard è sufficiente a garantire la regolare protezione antivirus del computer. L'utilizzo del database esteso può influire sulla velocità di funzionamento di Kaspersky Anti-Virus. Inoltre, alcuni dei programmi utilizzati potrebbero essere trattati come riskware.

Per selezionare il tipo di database antivirus da utilizzare con Kaspersky Anti-Virus,

1. seguire il collegamento Codici ostili ed esclusioni scansione nella sezione sinistra della scheda **Impostazioni** (vedere la figura 3).
2. Per utilizzare il database antivirus esteso, selezionare la casella **Adware, riskware, dialer automatici** nella sezione **Codici ostili rilevabili** della finestra di dialogo che verrà aperta. Per evitare la cancellazione di programmi che vengono utilizzati, si consiglia di selezionare, quale azione da eseguire al rilevamento di un oggetto pericoloso, un'azione che richieda la conferma dell'utente (vedere la sezione 5.2.2.2 a pagina 63).

La casella **Virus, worm, cavalli di troia, utilità di hacking, spyware** è selezionata per impostazione predefinita e non può essere deselezionata. Ciò indica che viene utilizzato il database antivirus standard per la scansione.

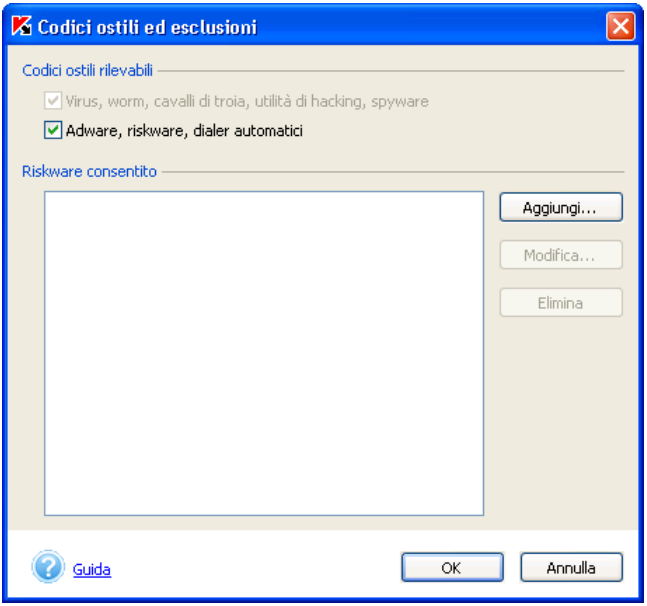

Figura 14. Selezione del tipo di database antivirus

5.2. Modalità di protezione in tempo reale

In modalità di protezione in tempo reale, Kaspersky Anti-Virus monitora costantemente tutte le chiamate agli oggetti del file system, la posta in arrivo ed in uscita e l'esecuzione di script VBScript e JavaScript potenzialmente pericolosi, delle macro utilizzate dalle applicazioni di Office e di programmi potenzialmente pericolosi.

Quando un utente o un programma aprono un oggetto per la scrittura/lettura, l'applicazione lo esamina alla ricerca di virus. Se viene rilevato un virus, l'applicazione cerca di disinfettare l'oggetto infetto, lo elimina o blocca l'accesso ad esso (secondo le impostazioni definite dall'utente). In tal modo, l'applicazione rileva ed elimina il codice ostile prima che il sistema venga infettato.

In modalità di protezione in tempo reale, l'applicazione esegue diverse funzioni:

- protezione dei file in tempo reale (vedere la sezione 5.2.1 a pagina 55);
- protezione della posta in tempo reale (vedere la sezione 5.2.2 a pagina 59);

- monitoraggio delle macro VBA (vedere la sezione 5.2.4 a pagina 65);
- monitoraggio degli script in tempo reale (vedere la sezione 5.2.5 a pagina 67);
- protezione in tempo reale contro gli attacchi di rete (vedere la sezione 5.2.6 a pagina 69);

Ciascuna delle funzioni suddette può essere configurata individualmente o disabilitata, senza conseguenze sul funzionamento di altri componenti del sistema di protezione in tempo reale del computer.

La parte destra della scheda **Protezione** della finestra principale dell'applicazione visualizza informazioni sullo stato corrente del sistema di protezione in tempo reale (vedere la figura 2).

Lo stato della protezione in tempo reale può essere indicato dalle seguenti icone:

protezione in tempo reale abilitata: le impostazioni corrispondono a quelle raccomandate;

protezione in tempo reale abilitata: le impostazioni non corrispondono però a quelle raccomandate;

protezione antivirus arrestata: questo stato indica che la protezione del computer è temporaneamente disabilitata;

protezione in tempo reale disattivata: in questo caso si consiglia di configurare le impostazioni della protezione in tempo reale e di avviarla.

La protezione in tempo reale è abilitata a partire dal caricamento del sistema operativo e finché il computer non viene spento. Tuttavia, a volte può essere necessario arrestare la protezione in tempo reale. Per fare ciò, aprire il menu di scelta rapida di Kaspersky Anti-Virus e selezionare la voce **Interrompi in protezione in tempo reale** (vedere la figura 1).

Poiché è sconsigliabile disabilitare completamente la protezione antivirus, Kaspersky Anti-Virus ne suggerirà la disattivazione temporanea.

Per disabilitare la modalità di protezione in tempo reale,

selezionare una delle seguenti opzioni nella finestra **Interruzione protezione in tempo reale** (vedere la Figura 15):

- **Tra 5/10/15 minuti** - la protezione sarà abilitata una volta trascorso il periodo specificato.

- **Alla prossima connessione di rete** - la protezione sarà abilitata immediatamente dopo la connessione del computer alla rete (questa opzione appare nell'elenco se non si è ancora connessi alla rete)
- **Al prossimo avvio di Kaspersky Anti-Virus** - la protezione verrà abilitata se si avvia l'applicazione dal menu **Start** → **Tutti i programmi**→ **Kaspersky Anti-Virus 5.0 for Windows Workstations** o dopo il riavvio del sistema (sempre che sia abilitato l'avvio automatico del programma all'avvio del sistema).
- **Solo manualmente** - la protezione può essere abilitata solo manualmente dall'utente. Per abilitare la protezione, selezionare la voce **Attiva protezione in tempo reale** dal menu di scelta rapida di Kaspersky Anti-Virus.

Interruzione Protezione in tempo reale
La protezione in tempo reale del computer è stata temporaneamente sospesa. Questo può provocare la penetrazione di virus nel computer.
Selezionare quando si desidera riattivare la protezione in tempo reale:
Tra
5 minuti
Al prossimo avvio di Kaspersky Anti-Virus
Solo manualmente
Non visualizzare questa finestra in futuro
Guida
OK
Annulla

Figura 15. Disabilitazione temporanea della protezione in tempo reale

La disabilitazione della modalità di protezione in tempo reale aumenta notevolmente il rischio di infezioni nel computer. Tuttavia, durante l'esecuzione di certe operazioni (ad esempio la deframmentazione di un disco con file system FAT32), la protezione in tempo reale può essere disabilitata per risparmiare tempo.

Se necessario, è anche possibile disabilitare alcuni dei componenti dell'applicazione anziché l'intero sistema di protezione: la protezione del file system (vedere la sezione 5.2.1 a pagina 55), la protezione della posta (vedere la sezione 5.2.2 a pagina 59), il monitoraggio delle macro (vedere la sezione 5.2.4 a pagina 65), il monitoraggio degli script (vedere la sezione 5.2.5 a pagina 67) o la protezione contro gli attacchi di rete (vedere la sezione 5.2.6 a pagina 69).

Per visualizzare o modificare le impostazioni della modalità di protezione in tempo reale:

seguire il collegamento Configura protezione in tempo reale nella sezione sinistra della scheda **Impostazioni** (vedere la figura 3).

La finestra della protezione in tempo reale contiene diverse schede, corrispondenti alle specifiche funzioni di protezione. Di seguito sono descritte in dettaglio le varie funzioni.

5.2.1. Scansione del file system

Nella modalità di protezione in tempo reale, Kaspersky Anti-Virus analizza tutte le chiamate al file system del computer, alla ricerca di codice ostile.

Il sistema di protezione file in tempo reale viene configurato nella scheda **File** della finestra **Impostazioni della protezione in tempo reale** (vedere la Figura 16). Questa finestra consente di:

- abilitare/disabilitare la protezione. Per fare ciò, selezionare o deselezionare la casella **Abilita protezione file in tempo reale**. Questa casella è selezionata per impostazione predefinita, abilitando la protezione;
- specificare il livello di protezione antivirus e configurare in dettaglio il livello selezionato (vedere la sezione 5.2.1.1 a pagina 56);
- creare un elenco di oggetti che non verranno esaminati in modalità di protezione file in tempo reale (vedere la sezione 5.7 a pagina 94). Per accedere alla finestra che consente di creare l'elenco delle esclusioni, scegliere i collegamenti non specificato/specificato accanto alle impostazioni di esclusione nella descrizione delle impostazioni di protezione specificate. L'aspetto del collegamento cambia in funzione della presenza o meno di esclusioni specificate;
- creare un elenco di processi attendibili le cui attività sui file non saranno monitorate nella modalità di protezione file in tempo reale (vedere la sezione 5.5 a pagina 91);
- specificare l'azione che verrà eseguita da Kaspersky Anti-Virus al rilevamento di oggetti pericolosi e sospetti (vedere la sezione 5.2.1.2 a pagina 58).

Figura 16. Impostazioni dell'attività di protezione degli oggetti del file system

5.2.1.1. Selezione del livello di protezione antivirus

Selezionare uno dei livelli predefiniti dagli esperti di Kaspersky Lab dall'elenco a discesa Impostazioni del livello di protezione (per maggiori dettagli vedere il Capitolo 4 a pagina 34). Per impostazione predefinita, saranno applicate le impostazioni del livello di protezione antivirus raccomandato.

È possibile configurare le proprie impostazioni sulla base delle impostazioni di qualsiasi livello di protezione. In questo caso, il livello di protezione passerà alla dicitura **Impostazioni definite dall'utente**. Tali impostazioni definite dall'utente non saranno salvate quando si torna alle impostazioni di uno dei tre livelli predefiniti.

È possibile visualizzare e modificare le impostazioni del livello di protezione selezionato nella finestra **Impostazione di protezione file in tempo reale** (vedere la Figura 17) che si apre scegliendo il pulsante **Impostazioni** nella scheda **File** (vedere la Figura 16).

Selezionare le caselle corrispondenti alle unità da esaminare nella sezione **Definizione scansione**.

Selezionare gli oggetti da includere nell'ambito della scansione nella sezione **Oggetti da esaminare**:

- **Esamina tutto** - esamina i file a prescindere dal tipo e dall'estensione.
- **Esamina solo gli oggetti che possono essere infetti** - esamina i file che possono essere potenzialmente infetti; l'analisi alla ricerca di virus viene eseguita in base alla struttura interna del file.
- **Esamina gli oggetti per estensione** - esamina i file che possono essere potenzialmente infetti; l'analisi alla ricerca di virus viene eseguita in base all'estensione del file.

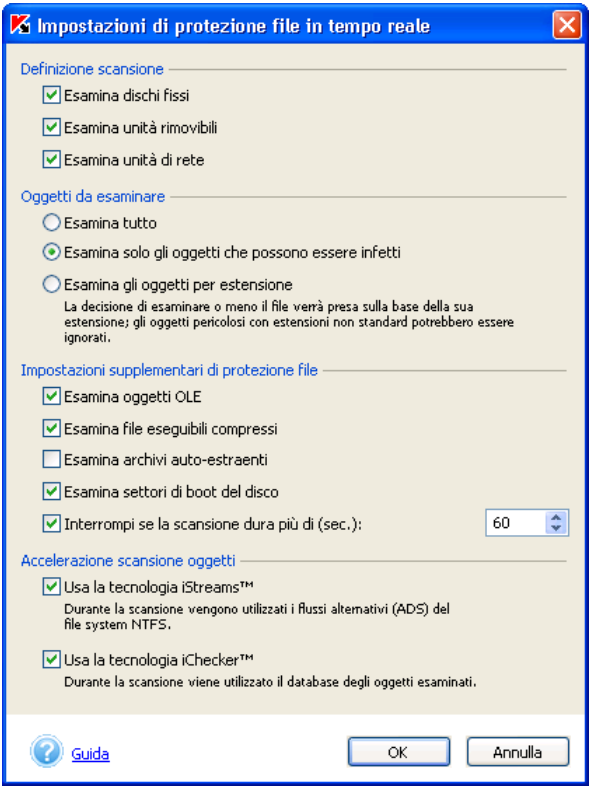
Impostazioni di protezione file in tempo reale
Definizione scansione
Esamina dischi fissi
Esamina unità rimovibili
Esamina unità di rete
Oggetti da esaminare
Esamina tutto
Esamina solo gli oggetti che possono essere infetti
Esamina gli oggetti per estensione
La decisione di esaminare o meno il file verrà presa sulla base della sua estensione; gli oggetti pericolosi con estensioni non standard potrebbero essere ignorati.
Impostazioni supplementari di protezione file
Esamina oggetti OLE
Esamina file eseguibili compressi
Esamina archivi auto-estraenti
Esamina settori di boot del disco
Interrompi se la scansione dura più di (sec.):
60
Accelerazione scansione oggetti
Usa la tecnologia iStreams™
Durante la scansione vengono utilizzati i flussi alternativi (ADS) del file system NTFS.
Usa la tecnologia iChecker™
Durante la scansione viene utilizzato il database degli oggetti esaminati.
Guida
OK
Annulla

Figura 17. Rifinitura della protezione dei file in tempo reale

È possibile limitare il tempo di scansione di un singolo oggetto nella sezione **Impostazioni supplementari di protezione file** specificando il valore dell'intervallo di scansione in secondi; è inoltre possibile specificare se esaminare o meno i seguenti oggetti:

- oggetti allegati o incorporati in altri file (*oggetti OLE*),
- file compressi eseguibili;
- archivi autoestraenti;
- settori di boot del disco.

La sezione **Accelerazione scansione oggetti** consente di abilitare/disabilitare l'utilizzo delle tecnologie di accelerazione della scansione antivirus: iChecker™ e iStreams™. Per fare ciò, selezionare le caselle corrispondenti.

5.2.1.2. Azioni da eseguire su un oggetto rilevato

Specificare l'azione che dovrà essere eseguita da Kaspersky Anti-Virus in caso di rilevamento di un oggetto pericoloso o sospetto nella sezione **Azioni da eseguire sugli oggetti rilevati** (vedere la Figura 16):

- **Richiedi intervento utente** - blocca l'accesso all'oggetto e visualizza una richiesta per l'azione da eseguire sull'oggetto. Questa è la modalità di funzionamento predefinita.

  Se l'applicazione non riceve istruzioni entro 30 secondi, sull'oggetto verrà eseguita l'azione raccomandata. Per ogni tipo di oggetto rilevato è disponibile la relativa azione raccomandata.

  Ecco un elenco di tutte le azioni possibili proposte da Kaspersky Anti-Virus (l'insieme di azioni può variare in funzione dell'oggetto specifico):

  - *Disinfetta l'oggetto infetto*
  - Metti in *Quarantena* l'oggetto potenzialmente infetto da virus o una sua modifica.

A volte, dopo aver messo un file in quarantena, può venire visualizzato un messaggio che comunica l'impossibilità di eliminare l'oggetto. Ciò ha a che vedere col fatto che mettere un oggetto in quarantena implica il suo spostamento: viene copiato in quarantena ed eliminato dalla posizione originale. Tuttavia, non tutti gli oggetti possono essere eliminati durante quest'operazione. Ad esempio, un oggetto attualmente utilizzato da un'altra applicazione non può essere eliminato.

- *Elimina oggetti infetti* che non è stato possibile o non è possibile disinfettare.
- *Ignora* - non viene eseguita alcuna azione sull'oggetto interessato. Il programma si limita a registrarne il rilevamento nell'apposito report.

- **Esegui l'azione raccomandata** - blocca l'accesso all'oggetto ed esegue su di esso l'azione raccomandata. L'azione raccomandata per gli oggetti infetti è *Disinfetta*, quella per gli oggetti potenzialmente infetti è metterli in *Quarantena*, mentre per i cavalli di troia e i worm è *Elimina*.
- **Blocca accesso ed elimina** - blocca l'oggetto e lo elimina senza ulteriori notifiche all'utente. Quando un oggetto viene eliminato, ne viene salvata una copia nella memoria di backup.
- **Blocca solo l'accesso** - blocca l'accesso all'oggetto, non visualizza richieste per l'elaborazione dell'oggetto e registra le informazioni nel report.
- **Quarantena** (solo per oggetti sospetti) - blocca l'accesso all'oggetto e lo sposta nella cartella della quarantena in attesa di esaminarlo con un database più aggiornato ed eventualmente ripristinarlo, oppure inviarlo a Kaspersky Lab per ulteriori analisi od eliminarlo.

5.2.2. Scansione della posta

In modalità di protezione in tempo reale, Kaspersky Anti-Virus analizza le richieste di ricezione e invio della posta elettronica, impedendo la penetrazione di codici ostili nella casella di posta nonché l'invio di oggetti sospetti o infetti agli indirizzi presenti in rubrica.

Kaspersky Anti-Virus esegue le seguenti funzioni:

- Intercettazione dei messaggi di posta elettronica in arrivo e in uscita tramite i protocolli SMTP e POP3 per qualsiasi client di posta;
- Intercettazione dei messaggi di posta elettronica in arrivo e in uscita in Microsoft Outlook tramite qualsiasi protocollo da questo utilizzato;
- rilevamento degli oggetti sospetti o infetti, sia nel corpo del messaggio che negli allegati, a qualsiasi livello di nidificazione.

Per impostazione predefinita, la scansione della posta elettronica viene eseguita in base alle impostazioni raccomandate; l'applicazione esamina quanto segue:

- messaggi di posta elettronica in arrivo tramite il protocollo POP3;
- archivi e file allegati nei formati di messaggio di posta.

Si noti che la posta in uscita inviata tramite il protocollo SMTP NON viene esaminata per impostazione predefinita.

Il sistema di protezione della posta in tempo reale viene configurato nella scheda **Posta** della finestra **Impostazioni della protezione in tempo reale** (vedere la Figura 18). Questa finestra consente di:

- abilitare/disabilitare la protezione. Per fare ciò, selezionare o deselezionare la casella **Abilita protezione posta in tempo reale**. Questa casella è selezionata per impostazione predefinita: la protezione è abilitata;
- specificare il livello di protezione antivirus e configurare in dettaglio il livello selezionato (vedere la sezione 5.2.1.1 a pagina 56);
- creare un elenco di oggetti che non verranno esaminati in modalità di protezione posta in tempo reale (vedere la sezione 5.7 a pagina 94). Per accedere alla finestra di creazione dell'elenco di esclusioni, scegliere il collegamento non specificato/specificato accanto alle impostazioni di esclusione nella descrizione delle impostazioni di protezione specificate. L'aspetto del collegamento cambia in funzione della presenza o meno di esclusioni specificate;
- specificare l'azione che verrà eseguita da Kaspersky Anti-Virus al rilevamento di oggetti pericolosi e sospetti (vedere la sezione 5.2.1.2 a pagina 58).

Uno speciale modulo integrato in Microsoft Outlook è stato implementato nel pacchetto per poterne esaminare i messaggi di posta elettronica. Quando viene installato Kaspersky Anti-Virus, nella finestra delle impostazioni di Microsoft Outlook viene visualizzata un'ulteriore scheda (per maggiori dettagli vedere la sezione 5.2.3 a pagina 64).

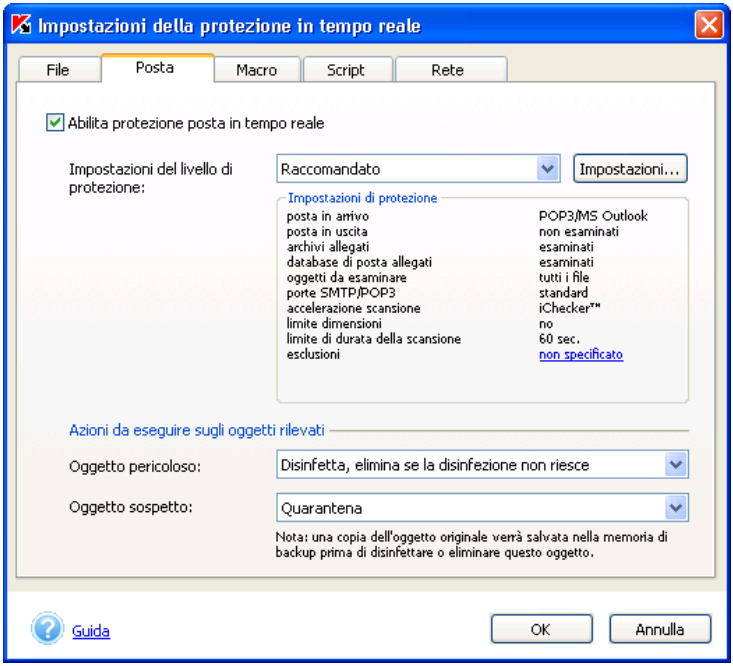

Figura 18. Impostazioni dell'attività di protezione posta

5.2.2.1. Selezione del livello di protezione antivirus

Selezionare uno dei livelli predefiniti dagli esperti di Kaspersky Lab dall'elenco a discesa **Impostazioni del livello di protezione** (per maggiori dettagli vedere il Capitolo 4 a pagina 34). Per impostazione predefinita, saranno applicate le impostazioni del livello di protezione antivirus raccomandato.

È possibile configurare le proprie impostazioni sulla base delle impostazioni di qualsiasi livello di protezione. In questo caso, il livello di protezione passerà alla dicitura **Impostazioni definite dall'utente**. Tali impostazioni definite dall'utente non saranno salvate quando si torna alle impostazioni di uno dei tre livelli predefiniti.

È possibile visualizzare e modificare le impostazioni del livello di protezione selezionato nella finestra **Impostazione di protezione posta in tempo reale** (vedere la Figura 19) che si apre scegliendo il pulsante **Impostazioni** nella scheda **Posta** (vedere la Figura 18).

Le caselle utilizzate per decidere quali oggetti sottoporre a scansione sono ubicate nella parte superiore della finestra. Se la casella è selezionata, l'applicazione intercetta ed esamina gli oggetti corrispondenti:

- **Esamina posta ricevuta tramite il protocollo POP3** - esamina i messaggi di posta elettronica in arrivo tramite il protocollo POP3, per qualsiasi client di posta.
- **Esamina posta in arrivo di Microsoft Outlook** - esamina la posta di Microsoft Outlook in arrivo tramite qualsiasi protocollo di posta.
- **Esamina posta inviata tramite il protocollo SMTP** - esamina i messaggi di posta elettronica in uscita tramite il protocollo SMTP, per qualsiasi client di posta.
- **Esamina posta in uscita di Microsoft Outlook** - esamina la posta di Microsoft Outlook in uscita tramite qualsiasi protocollo di posta.
- **Esamina archivi allegati** - esamina gli archivi allegati ai messaggi di posta.

  Si noti che l'esclusione degli archivi allegati dalla scansione non influisce sulla scansione degli archivi autoestraenti, che vengono sempre esaminati a qualsiasi livello di nidificazione.
- **Esamina database di posta allegati** - esamina i database di posta allegati.

La sezione **Impostazioni porte** consente di determinare i valori delle porte di posta POP3 e SMTP, utilizzate per trasferire i dati. Per impostazione predefinita, vengono utilizzate le porte 110 e 25. Se il client di posta utilizzato lavora con porte diverse, specificarne il valore.

Inoltre, è possibile imporre delle restrizioni sul tempo di scansione di un oggetto e le sue dimensioni:

- **Non esaminare messaggi superiori a (MB):** - specificare le dimensioni massime degli oggetti da esaminare, in MB, per limitarle ad un certo valore.
- **Interrompi se la scansione dura più di (sec.):** - specificare l'intervallo di scansione in secondi per limitarlo ad un certo valore.

La sezione **Accelerazione scansione oggetti** consente di abilitare/disabilitare l'utilizzo della tecnologia di accelerazione della scansione antivirus iChecker™. Per utilizzare questa tecnologia, selezionare la casella **Usa la tecnologia iChecker™** .

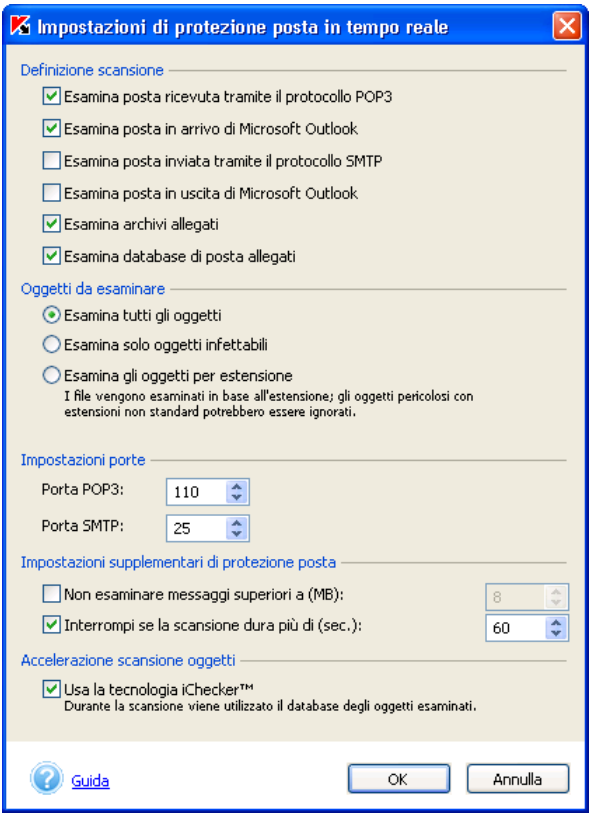
Impostazioni di protezione posta in tempo reale
Definizione scansione
Esamina posta ricevuta tramite il protocollo POP3
Esamina posta in arrivo di Microsoft Outlook
Esamina posta inviata tramite il protocollo SMTP
Esamina posta in uscita di Microsoft Outlook
Esamina archivi allegati
Esamina database di posta allegati
Oggetti da esaminare
Esamina tutti gli oggetti
Esamina solo oggetti infettabili
Esamina gli oggetti per estensione
I file vengono esaminati in base all'estensione; gli oggetti pericolosi con estensioni non standard potrebbero essere ignorati.
Impostazioni porte
Porta POP3: 110
Porta SMTP: 25
Impostazioni supplementari di protezione posta
Non esaminare messaggi superiori a (MB): 8
Interrompi se la scansione dura più di (sec.): 60
Accelerazione scansione oggetti
Usa la tecnologia iChecker™
Durante la scansione viene utilizzato il database degli oggetti esaminati.
Guida
OK
Annulla

Figura 19. Rifinitura delle impostazioni di scansione della posta

5.2.2.2. Azioni da eseguire su un oggetto rilevato

Nella sezione **Azioni da eseguire sugli oggetti rilevati**, scegliere il tipo di azione da eseguire in caso di rilevamento di un oggetto infetto o sospetto:

- *Disinfetta, elimina se la disinfezione non riesce* - l'applicazione cercherà di disinfettare l'oggetto infetto; se ciò non è possibile, l'oggetto sarà eliminato.
- *Quarantena* - gli oggetti sospetti vengono trasferiti nella cartella della quarantena in attesa di essere esaminati con database antivirus più aggiornati, oppure ripristinati, inviati a Kaspersky Lab per ulteriori analisi o eliminati.

- *Elimina* - elimina l'oggetto infetto. Se si seleziona questa azione, dell'oggetto eliminato verrà creata una copia che sarà archiviata nella cartella di backup. La copia potrà essere utilizzata per ripristinare il file, oppure inviata a Kaspersky Lab per ulteriore analisi.

5.2.3. Scansione della posta di Microsoft Outlook

La posta di Microsoft Outlook viene esaminata tramite uno speciale modulo integrato nel programma stesso. Tale modulo è stato studiato per esaminare tutta la posta in arrivo (messaggi ed allegati) prima di leggerla, e quella in uscita prima di inviarla.

Per aprire la finestra di scansione della posta elettronica, selezionare **Strumenti →Opzioni…** dal menu principale di Microsoft Outlook. Nella finestra **Opzioni**, aprire la scheda **Kaspersky Anti-Virus** (vedere la Figura 20).

La sezione **Stato** visualizza lo stato del modulo di scansione della posta elettronica. A seconda della sua condizione possono essere visualizzati i seguenti messaggi:

- *La scansione della posta in entrata e in uscita è abilitata*. Questo messaggio viene visualizzato quando Kaspersky Anti-Virus è in esecuzione e la funzione di scansione della posta di Microsoft Outlook è abilitata.
- *La scansione della posta in entrata è abilitata*. Questo messaggio viene visualizzato quando è abilitata la scansione dei soli messaggi in entrata.
- *La scansione della posta in uscita è abilitata*. Questo messaggio viene visualizzato quando è abilitata la scansione dei soli messaggi in uscita.
- *La scansione della posta è disattivata*. Questo messaggio viene visualizzato quando la scansione dei messaggi di Microsoft Outlook in entrata ed in uscita è disabilitata, oppure se Kaspersky Anti-Virus non è in esecuzione.

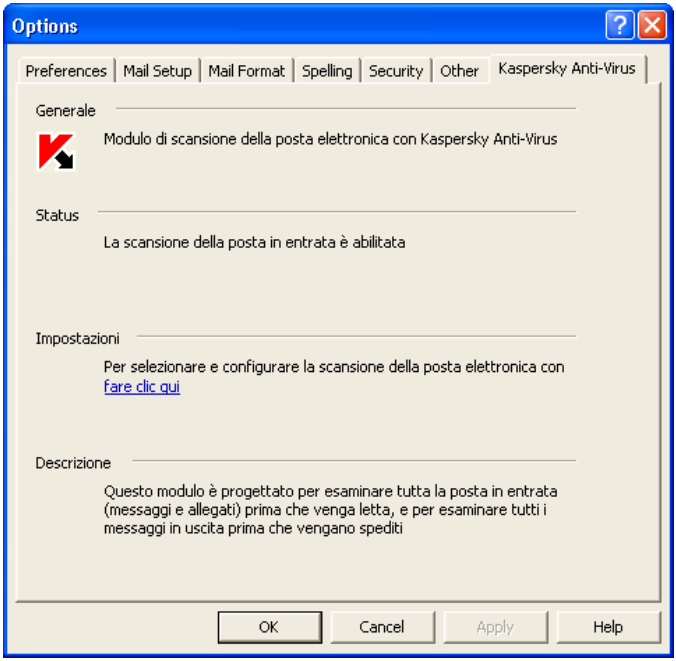
Options
Preferences
Mail Setup
Mail Format
Spelling
Security
Other
Kaspersky Anti-Virus
Generale
Modulo di scansione della posta elettronica con Kaspersky Anti-Virus
Status
La scansione della posta in entrata è abilitata
Impostazioni
Per selezionare e configurare la scansione della posta elettronica con fare clic qui
Descrizione
Questo modulo è progettato per esaminare tutta la posta in entrata (messaggi e allegati) prima che venga letta, e per esaminare tutti i messaggi in uscita prima che vengano spediti
OK
Cancel
Apply
Help

Figura 20. La scheda Kaspersky Anti-Virus in Microsoft Outlook

Per configurare la scansione della posta elettronica, utilizzare il collegamento fare clic qui nella sezione **Impostazioni**. Ciò aprirà le impostazioni della protezione in tempo reale nella scheda **Posta** (vedere la Figura 18).

La finestra delle impostazioni della protezione in tempo reale si aprirà solo se è selezionata la casella **Visualizza interfaccia utente** nella scheda **Generale** (vedere la Figura 58) della finestra delle impostazioni supplementari di Kaspersky Anti-Virus.

Gli utenti di workstation possono visualizzare solo lo stato **La scansione della posta è abilitata/disattivata** nella scheda **Kaspersky Anti-Virus** (vedere la Figura 20). La sezione Impostazioni non è accessibile.

5.2.4. Monitoraggio delle macro

Nella modalità di protezione in tempo reale, se il monitoraggio delle macro e abilitato, Kaspersky Anti-Virus analizza un insieme di comandi macro VBA e ne previene l'esecuzione.

Il monitoraggio delle macro viene configurato nella scheda **Macro** della finestra **Impostazioni della protezione in tempo reale** (vedere la Figura 21).

Il monitoraggio delle macro è abilitato per impostazione predefinita. Per disabilitare il monitoraggio, deselezionare la casella **Abilita monitoraggio macro VBA in tempo reale**.

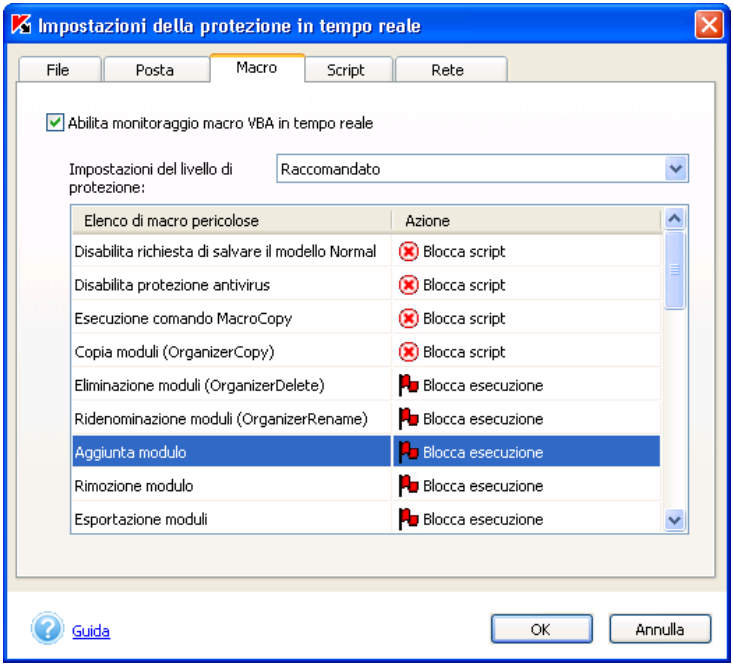

Figura 21. Impostazioni dell'attività di monitoraggio delle macro

Selezionare uno dei livelli predefiniti dagli esperti di Kaspersky Lab dall'elenco a discesa **Impostazioni del livello di protezione** (per maggiori dettagli vedere il Capitolo 4 a pagina 34).

La seguente tabella contiene l'elenco di macro sospette monitorate dall'applicazione, nonché le azioni previste per ciascun tipo di macro in funzione del livello di protezione.

Consenti esecuzione - consente l'esecuzione delle macro senza eseguire alcuna azione.

Richiedi azione - richiede l'azione da eseguire. La richiesta elenca tutte le azioni che possono essere eseguite per questa macro.

Blocca esecuzione - blocca l'esecuzione della macro.

Blocca script - interrompe l'esecuzione dello script che ha richiamato la macro.

È possibile configurare le proprie impostazioni sulla base delle impostazioni di qualsiasi livello di protezione. In questo caso, il livello di protezione passerà alla dicitura **Impostazioni definite dall'utente**. Tali impostazioni definite dall'utente non saranno salvate quando si torna alle impostazioni di uno dei tre livelli predefiniti.

Per cambiare l'azione che verrà eseguita da Kaspersky Anti-Virus al rilevamento di una macro sospetta,

Selezionare una cella corrispondente alla macro nella colonna **Azione** della tabella, quindi selezionare una delle azioni dall'elenco a discesa.

5.2.5. Monitoraggio degli script

In modalità di protezione in tempo reale, se è abilitato il monitoraggio degli script in tempo reale, Kaspersky Anti-Virus analizzerà gli script VBScript e JavaScript prima della loro esecuzione tramite il modulo di elaborazione script del sistema operativo, e impedirà l'esecuzione di codice ostile.

Le impostazioni di monitoraggio degli script vengono configurate nella scheda **Script** della finestra **Impostazioni della protezione in tempo reale** (vedere la Figura 22).

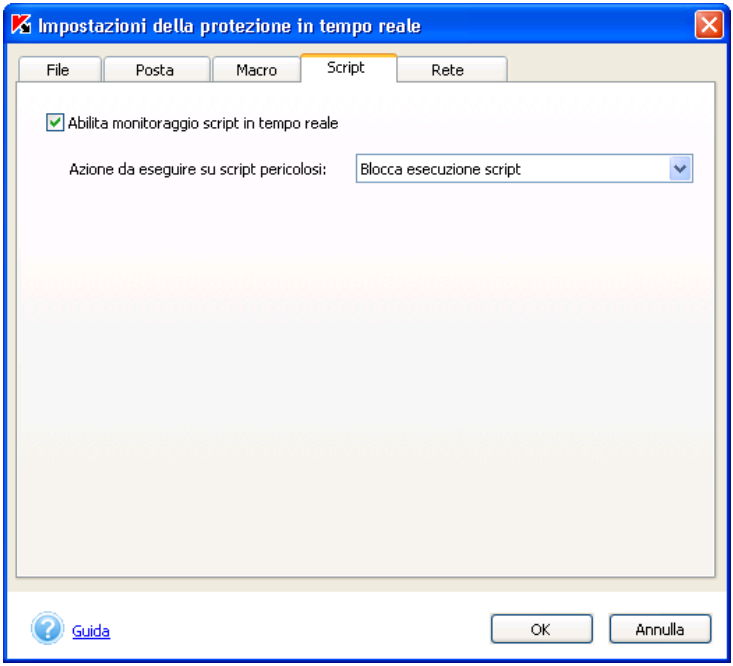

Figura 22. Impostazioni dell'attività di monitoraggio degli script

Il monitoraggio degli script è abilitato per impostazione predefinita. Per disabilitare il monitoraggio, deselezionare la casella **Abilita monitoraggio script in tempo reale** .

Per cambiare l'azione che verrà eseguita da Kaspersky Anti-Virus al rilevamento di una macro sospetta:

- **Richiedi intervento utente** - visualizza un avviso relativo al rilevamento di uno script potenzialmente nocivo e richiede l'intervento dell'utente. La richiesta elenca tutte le azioni che possono essere eseguite.
- **Blocca esecuzione script** - blocca l'esecuzione dello script.
- **Consenti esecuzione script** - consente l'esecuzione dello script.

Durante la scansione dello script, la barra di stato di Microsoft Internet Explorer visualizza l'icona di Kaspersky Anti-Virus che lampeggia.

5.2.6. Protezione contro gli attacchi di rete

Kaspersky Anti-Virus consente di proteggere il computer dagli attacchi dei pirati informatici provenienti dalla LAN o da Internet.

Gli attacchi dei pirati informatici vengono rilevati utilizzando il database degli attacchi attualmente conosciuti. Questo database viene aggiornato e installato con il database antivirus (per dettagli, vedere 5.1 a pagina 39).

La protezione contro gli attacchi di rete viene lanciata all'avvio di Kaspersky Anti-Virus, ed esamina tutti i dati ricevuti dalla rete a prescindere dall'origine: la LAN o internet.

Quando il computer viene attaccato, tale tentativo verrà bloccato. Sullo schermo verrà visualizzata una corrispondente notifica (vedere la Figura 23) contenente informazioni sul tipo di attacco, l'indirizzo IP del computer attaccante e la porta locale (se possibile).

Le impostazioni di protezione contro gli attacchi di rete vengono configurate nella scheda **Rete** della finestra **Impostazioni della protezione in tempo reale** (vedere la Figura 24).

L'abilitazione/disabilitazione della protezione in tempo reale tramite il menu di scelta rapida dall'icona di Kaspersky Anti-Virus (vedere la sezione 5.2 a pagina 52) nell'area di notifica abilita/disabilita anche la protezione contro gli attacchi di rete.

Per disabilitare solo la protezione contro gli attacchi di rete senza disabilitare altre attività di protezione in tempo reale, deselezionare la casella **Abilita la protezione in tempo reale contro gli attacchi di rete** (vedere la Figura 24). L'abilitazione/disabilitazione della protezione richiede il riavvio del computer.

Kaspersky Anti-Virus for Windows Workstations
Attenzione! Il computer ha subito un attacco da Internet.
L'attacco di rete ICMP Flood dall'indirizzo 10.0.0.1 è stato respinto.
Non mostrare più il messaggio in questa sessione
Guida
Audio OFF
OK

Figura 23. Notifica degli attacchi di rete

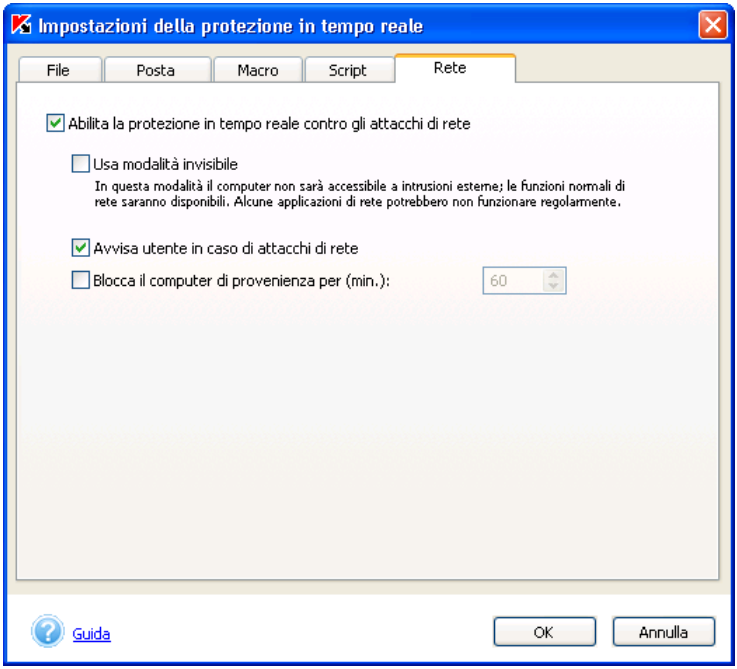
Impostazioni della protezione in tempo reale
File
Posta
Macro
Script
Rete
Abilita la protezione in tempo reale contro gli attacchi di rete
Usa modalità invisibile
In questa modalità il computer non sarà accessibile a intrusioni esterne; le funzioni normali di rete saranno disponibili. Alcune applicazioni di rete potrebbero non funzionare regolarmente.
Avvisa utente in caso di attacchi di rete
Blocca il computer di provenienza per (min.):
60
Guida
OK
Annulla

Figura 24. Rifinitura della protezione in tempo reale contro gli attacchi di rete

È possibile definire le seguenti impostazioni per il funzionamento di Kaspersky Anti-Virus in modalità di protezione della rete in tempo reale:

- *Modalità invisibile:* Questa modalità permette solo le attività di rete avviate dall'utente o da un'applicazione installata sul computer dell'utente, mentre tutte le altre attività (connessione remota al computer, ecc.) non saranno consentite. Ciò significa che il computer diventa praticamente "invisibile" per l'ambiente esterno. Inoltre, la modalità invisibile aiuta a prevenire qualsiasi tipo di attacco DoS (Denial of Service). Allo stesso tempo, la modalità invisibile non ha effetti negativi sulla velocità di navigazione in Internet: Kaspersky Anti-Virus consente tutte le attività di rete avviate dall'utente.

  Attenzione! La modalità invisibile non protegge il computer dai cavalli di troia!

  La modalità invisibile è disabilitata per impostazione predefinita. Per abilitarla, selezionare la casella **Usa modalità invisibile**.

- *Notifica degli attacchi di rete* Per impostazione predefinita, l'applicazione notifica qualsiasi tentativo di attacco al computer. Verrà visualizzato un

messaggio sul monitor (vedere la Figura 23) per notificare il tipo di attacco lanciato, l'indirizzo IP di provenienza dell'attacco, e su quale porta locale (se è stato possibile determinarlo). Poiché tale notifica viene fornita a fini esclusivamente informativi, è possibile disabilitarne la visualizzazione deselezionando la casella **Avvisa utente in caso di attacchi di rete**, ma le informazioni sugli attacchi vengono comunque registrate nei report.

- *Blocco del computer di provenienza.* Kaspersky Anti-Virus è in grado di bloccare tutti i computer da cui è stato lanciato il tentativo di attacco. Per impostazione predefinita, il blocco del computer di provenienza è disabilitato. Se si decide di abilitare tale modalità, il tempo di blocco predefinito sarà di 60 minuti. Per questo intervallo, tutti i pacchetti inviati al proprio computer da quello attaccante verranno bloccati. Per modificare il tempo di blocco, specificare il valore corrispondente per il parametro **Blocca il computer di provenienza per (min.):**. Per disabilitare la modalità di blocco, deselezionare la casella accanto a tale impostazione.

5.3. La modalità di scansione manuale

La *scansione manuale* è la modalità dell'applicazione mirata alla ricerca di codici ostili su richiesta dell'utente o dell'amministratore della workstation, ed alla successiva disinfezione o eliminazione degli oggetti infetti e messa in quarantena di quelli sospetti.

Kaspersky Anti-Virus consente la scansione completa del computer o delle sue componenti - singoli dischi o file, cartelle singole, caselle di posta. La scansione implica la disinfezione e l'eliminazione degli oggetti pericolosi rilevati, nonché la messa in quarantena di quelli sospetti.

Le seguenti attività di scansione manuale del sistema verranno create per impostazione predefinita durante l'installazione dell'applicazione:

- **Esamina le risorse del computer** - la scansione completa dell'intero file system del computer dell'utente (vedere la sezione 5.3.1 a pagina 72) viene lanciata automaticamente ogni venerdì alle 20:00.
- **Esamina le unità rimovibili** - per impostazione predefinita, la scansione dei supporti rimovibili (dischi floppy, CD, schede flash, ecc.) viene lanciata manualmente dall'utente (vedere la sezione 5.3.5 a pagina 86).
- **Esamina le aree critiche** - per impostazione predefinita, la scansione dalla memoria del sistema, degli oggetti di avvio, dei settori di boot del disco e delle cartelle di sistema *Windows* e *Windows/System32* viene lanciata manualmente dall'utente.

- **Esamina oggetti in quarantena** - per impostazione predefinita, la scansione degli oggetti in quarantena viene lanciata manualmente dall'utente.
- **Esegui la scansione all'avvio del sistema** - per impostazione predefinita, la scansione degli oggetti d'avvio, dalla memoria del sistema e dei settori di boot del disco viene lanciata automaticamente all'avvio del sistema.

È inoltre possibile specificare la scansione di un singolo oggetto (per dettagli, vedere la sezione 5.3.2 a pagina 73). Inoltre, è possibile creare ulteriori attività di scansione manuale di oggetti (vedere la sezione 5.6 a pagina 93).

Per disinfettare con successo i database di posta di Microsoft Outlook Express, è necessario chiudere il programma prima di eseguire la scansione.

5.3.1. Scansione completa del computer

La scansione completa consente di esaminare molti più oggetti che con la protezione in tempo reale; è consigliabile quindi eseguire la scansione completa del computer almeno una volta alla settimana, a fini preventivi.

L'applicazione notificherà quando è giunto il momento di eseguire la scansione completa. Se la finestra principale dell'applicazione è chiusa, verrà visualizzato un messaggio sopra l'icona di Kaspersky Anti-Virus nell'area di notifica, che consiglierà di avviare la scansione (sempre che la visualizzazione di tali messaggi non sia disabilitata, vedere la sezione 5.10.4 a pagina 114).

Per visualizzare maggiori dettagli, aprire la finestra principale dell'applicazione sulla scheda **Protezione** (vedere la figura 2) e osservare lo stato della scansione completa nella sezione destra della finestra. Lo stato della scansione completa può essere uno dei seguenti:

la scansione viene eseguita regolarmente o è attualmente in corso;

è necessario lanciare la scansione; è possibile che sia necessario tornare alle impostazioni raccomandate dagli esperti di Kaspersky Lab;

è necessario *eseguire immediatamente una scansione completa del computer.*

Se necessario, è possibile lanciare subito la scansione completa del computer dalla sezione che ne indica lo stato seguendo il collegamento eseguire la scansione completa del computer.

Gli esperti di Kaspersky Lab raccomandano di abilitare la modalità di scansione completa pianificata. Lo stato della scansione completa comprende informazioni sulla pianificazione o meno di quest'attività.

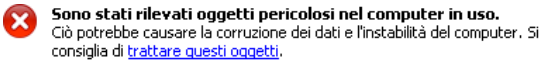
Sono stati rilevati oggetti pericolosi nel computer in uso.
Ciò potrebbe causare la corruzione dei dati e l'instabilità del computer. Si consiglia di trattare questi oggetti.

Figura 25. Informazioni sullo stato di scansione

*Per lanciare una scansione antivirus manuale, selezionare le seguenti voci nella parte sinistra della scheda **Protezione**:*

Esamina le risorse del computer lancia una scansione completa del computer in base alle impostazioni correnti (vedere di seguito). Si può raggiungere lo stesso risultato tramite il collegamento eseguire la scansione completa del computer nella parte destra della scheda **Protezione** e la voce **Cerca virus nel computer** dal menu visualizzato facendo clic col tasto destro del mouse sull'icona nell'area di notifica.

A questo punto si aprirà la finestra **Scansione in corso...** (vedere la Figura 5) che visualizza l'avanzamento dell'esecuzione dell'attività in percentuale, il nome dell'oggetto attualmente esaminato, il tempo stimato per il completamento della scansione e le informazioni statistiche generali contenenti il numero di oggetti esaminati, disinfettati, eliminati e messi in quarantena fino a questo punto.

La scansione completa del computer non comprende l'analisi delle caselle di posta né delle unità rimovibili e di rete, se ci sono unità di questo tipo collegate al computer.

È possibile nascondere la finestra di scansione scegliendo il pulsante nell'angolo superiore destro e selezionando **Chiudi la finestra e riprendi la scansione** nella finestra che verrà aperta.

I risultati della scansione sono visualizzabili nel report (per dettagli, vedere la sezione 5.10.2 a pagina 109).

5.3.2. Scansione degli oggetti selezionati

È possibile selezionare un oggetto da esaminare utilizzando l'interfaccia di Kaspersky Anti-Virus o gli strumenti standard di Windows (ad esempio, il **desktop** o **Esplora risorse**, ecc.)

Per selezionare un oggetto da esaminare utilizzando l'interfaccia di Kaspersky Anti-Virus,

seguire il collegamento Esamina oggetti nella sezione sinistra della scheda **Protezione** (vedere la figura 2).

La finestra **Seleziona oggetti da esaminare** (vedere la Figura 26) contiene l'elenco di oggetti che possono essere esaminati, e di pulsanti per modificare l'elenco e controllare la scansione.

L'elenco iniziale include già alcuni oggetti.

- unità rimovibili (compresi floppy disk e CD);
- dischi rigidi;
- unità di rete (se ci sono unità di questo tipo collegate al computer);
- caselle di posta di Microsoft Outlook e Microsoft Outlook Express;
- Cartella **Documenti**;
- memoria di sistema;
- oggetti di avvio;
- settori di boot del disco.

Figura 26. Selezione degli oggetti da esaminare

Se si desidera aggiungere un nuovo oggetto all'elenco, scegliere il pulsante **Aggiungi** e specificare il file o la cartella richiesta nella finestra che verrà visualizzata. Tutti gli oggetti aggiunti all'elenco verranno salvati per le scansioni successive.

Quando si crea un percorso ad una cartella o ad un oggetto, è possibile utilizzare le variabili di ambiente del sistema. Ad esempio, è possibile selezionare la scansione della cartella di installazione di Windows specificando la variabile **%windir%** .

Per eliminare un oggetto dall'elenco, selezionarlo e scegliere il pulsante **Elimina**. Tuttavia, si tenga presente che è possibile eliminare dall'elenco solo gli oggetti aggiunti manualmente. Gli oggetti inclusi originariamente nell'elenco non possono essere eliminati.

Per modificare le impostazioni utilizzate per eseguire la scansione degli oggetti selezionati, utilizzare il pulsante **Configura...** (per dettagli, vedere la sezione 5.3.3 a pagina 76). Le impostazioni immesse verranno salvate per la futura scansione degli oggetti inclusi nell'elenco e per la scansione degli oggetti selezionati utilizzando gli strumenti standard di Windows.

Per esaminare alcuni oggetti dall'elenco,

1. selezionare gli oggetti dall'elenco stesso.
2. Scegliere il pulsante **Scansione** per lanciare la scansione.

Per lanciare la scansione degli oggetti selezionati tramite gli strumenti standard di Windows,

Selezionare l'oggetto col mouse, fare clic col tasto destro per aprire il menu di scelta rapida di Windows e selezionare la voce **Scansione antivirus** (vedere la Figura 27). Per la scansione, verranno utilizzate le impostazioni specificate nella finestra **Seleziona oggetti da esaminare** (vedere la Figura 26).

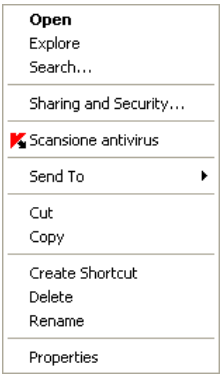

Figura 27. Scansione degli oggetti selezionati utilizzando gli strumenti di Windows

Se Kaspersky Anti-Virus non è in esecuzione, quando si lancia la scansione degli oggetti selezionandoli tramite gli strumenti di Windows viene proposto il lancio dell'applicazione.

A prescindere dal metodo utilizzato per avviare la scansione dell'oggetto (dal menu di scelta rapida di Windows o dall'elenco di oggetti di Kaspersky Anti-Virus), verrà visualizzata una finestra **Scansione in corso...** (vedere la Figura 5). I risultati della scansione sono visualizzabili nel report (per dettagli, vedere la sezione 5.10.2 a pagina 109).

Se alcuni oggetti vengono esaminati regolarmente, è possibile creare una corrispondente attività di scansione manuale (per dettagli, vedere la sezione 5.6 a pagina 93).

5.3.3. Configurazione della scansione manuale

Per visualizzare o modificare le impostazioni della scansione manuale,

seguire il collegamento Attività di scansione manuale nella sezione sinistra della scheda **Impostazioni** (vedere la figura 3).

Si aprirà la finestra **Attività di scansione manuale** (vedere la Figura 28), contenente l'elenco delle attività di sistema e quello delle attività di scansione supplementari create dall'utente.

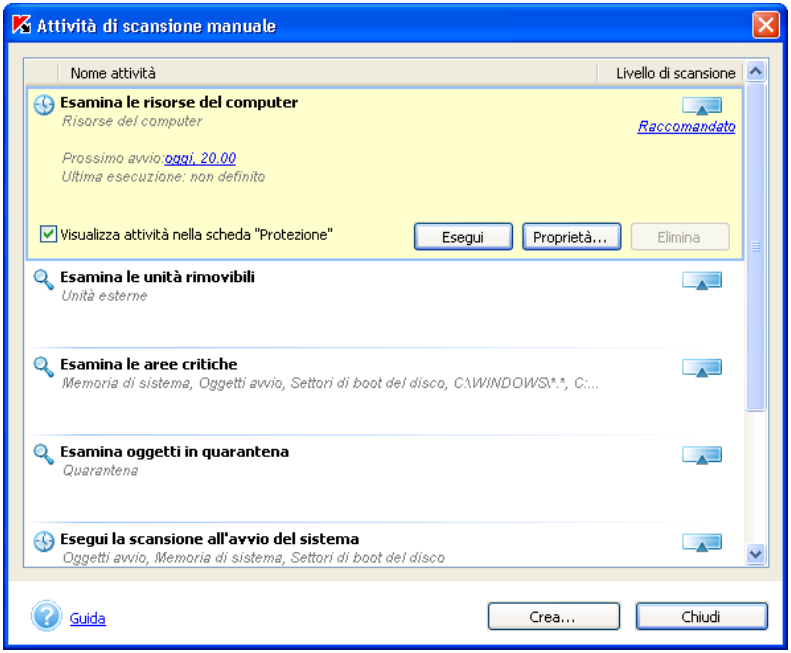

Figura 28. Elenco delle attività di scansione manuale

Il blocco contenente informazioni sulla definizione della scansione e l'ora di avvio dell'ultima e della prossima scansione si apre facendo clic sul nome dell'attività. Questo blocco consente di lanciare una scansione manuale utilizzando il pulsante **Esegui**, o di aprire la finestra di configurazione delle impostazioni della scansione antivirus (vedere la Figura 29), che consente di:

- selezionare gli oggetti da esaminare; è possibile aggiungere oggetti solo alle attività create manualmente. Per aggiungere un nuovo oggetto, scegliere il pulsante **Aggiungi...** e selezionare quello desiderato dall'elenco a discesa. Per esaminare un oggetto non compreso nell'elenco, ad esempio una singola cartella o un singolo file, selezionare la voce **Sfoglia...** dall'elenco e specificare il percorso a questo oggetto. Per eliminare un oggetto dall'elenco di oggetti da esaminare, selezionarlo dall'elenco e scegliere il pulsante **Elimina**;
- specificare il livello di protezione antivirus e configurare in dettaglio il livello selezionato (vedere la sezione 5.3.3.1 a pagina 79);
- creare un elenco di oggetti che non saranno esaminati (vedere la sezione 5.7 a pagina 94). Per accedere alla finestra che consente di creare l'elenco delle esclusioni, scegliere il collegamento non

specificato/specificato accanto alla descrizione delle impostazioni di protezione selezionate. L'aspetto del collegamento cambia in funzione della presenza o meno di esclusioni specificate;

- selezionare l'azione che verrà utilizzata da Kaspersky Anti-Virus al rilevamento di oggetti pericolosi e sospetti (vedere la sezione 5.3.3.2 a pagina 82).
- pianificare il lancio automatico delle attività di scansione (vedere la sezione 5.7 a pagina 94);
- configurare l'avvio dell'attività con un diverso account utente (solo per computer che eseguono Microsoft Windows NT/2K/XP) (vedere la sezione 5.9 a pagina 101);

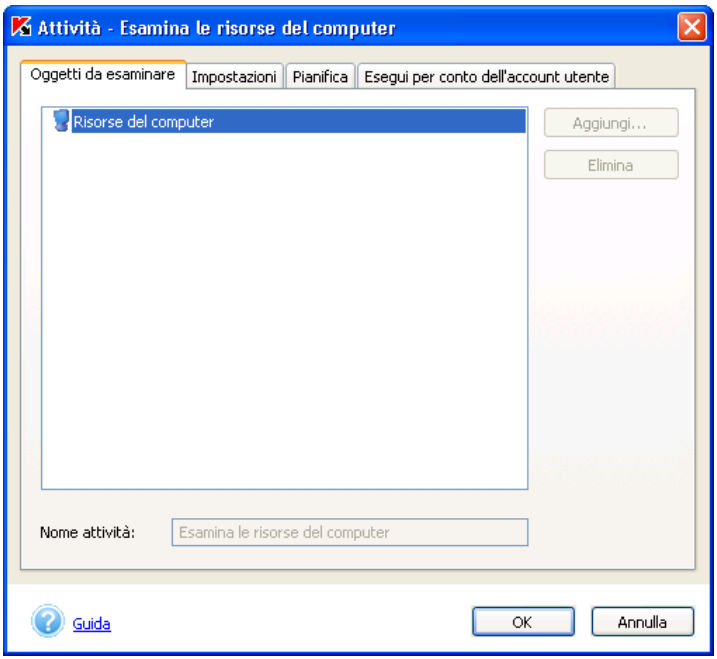

Figura 29. Finestra Impostazioni della scansione manuale La scheda **Oggetti da esaminare**

Se si prevede di lanciare un'attività frequentemente, si raccomanda di selezionare la casella **Visualizza attività nella scheda "Protezione"**, nella sezione informativa del blocco. In tal caso, sarà possibile lanciare tale attività facendo clic sul collegamento con il suo nome, ubicato nella sezione sinistra della scheda **Protezione** (vedere la figura 2).

A seconda della situazione, a sinistra del nome dell'attività può comparire una delle seguenti icone:

- questa icona indica che questa attività è stata pianificata, in modo da poter essere eseguita automaticamente.

– indica che l'attività è in esecuzione.

Per creare un'attività di scansione aggiuntiva, utilizzare il pulsante **Crea...** nella finestra **Attività di scansione manuale** (vedere la Figura 28). Per dettagli sulla creazione dell'attività, vedere la sezione 5.6 a pagina 93).

Per eliminare l'attività, selezionarla dall'elenco e scegliere il pulsante **Elimina**. Tuttavia, si tenga presente che è possibile eliminare dall'elenco solo le attività aggiunte manualmente. È impossibile eliminare le attività di sistema. Inoltre, è impossibile eliminare le attività che sono in esecuzione al momento.

5.3.3.1. Selezione del livello di scansione

Selezionare uno dei livelli predefiniti dagli esperti di Kaspersky Lab (vedere la Figura 30) dall'elenco a discesa **Impostazioni del livello di scansione** della scheda **Impostazioni** (vedere la sezione Capitolo 4 a pagina 34). Per impostazione predefinita, saranno applicate le impostazioni del livello di scansione antivirus raccomandato.

È possibile configurare le proprie impostazioni sulla base delle impostazioni di qualsiasi livello. In questo caso, il livello di protezione passerà alla dicitura **Impostazioni definite dall'utente**. Tali impostazioni definite dall'utente non saranno salvate quando si torna alle impostazioni di uno dei tre livelli predefiniti.

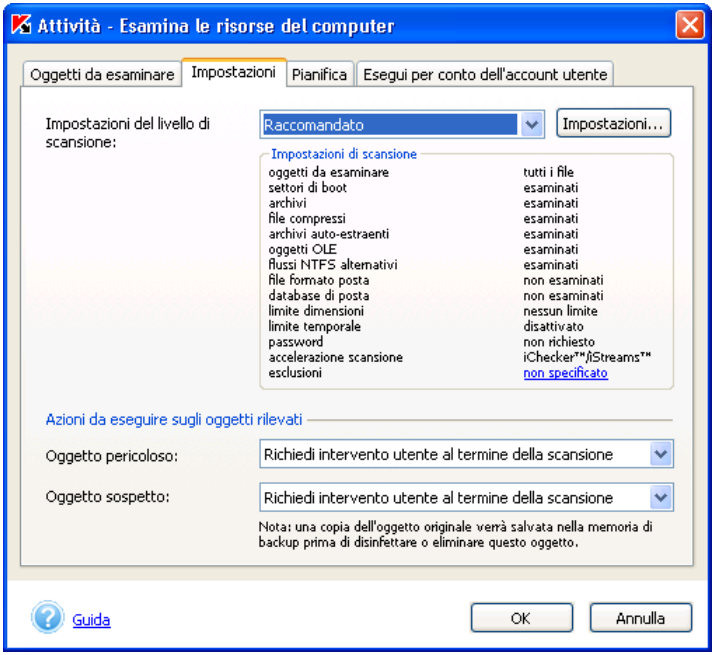

Figura 30. Configurazione di una scansione manuale

È possibile visualizzare e modificare le impostazione del livello selezionato nella finestra **Impostazioni della scansione manuale** (vedere la Figura 31) che si apre scegliendo il pulsante **Impostazioni** (vedere la Figura 30).

Selezionare i tipi di oggetti da esaminare nella sezione **Oggetti da esaminare**:

- **Esamina tutto** - esamina i file a prescindere dal tipo e dall'estensione.
- **Esamina solo gli oggetti che possono essere infetti** - esamina i file che possono essere potenzialmente infetti; l'analisi alla ricerca di virus viene eseguita in base alla struttura interna del file.
- **Esamina gli oggetti per estensione** - esamina i file che possono essere potenzialmente infetti; l'analisi alla ricerca di virus viene eseguita in base all'estensione del file.

La sezione **Impostazioni supplementari di scansione** consente di specificare se esaminare o meno i seguenti oggetti:

- settori di boot;
- archivi;

- file compressi eseguibili;
- archivi autoestraenti;
- oggetti allegati o incorporati in altri file (*oggetti OLE*);
- flussi NTFS supplementari;
- file di posta;
- database di posta.

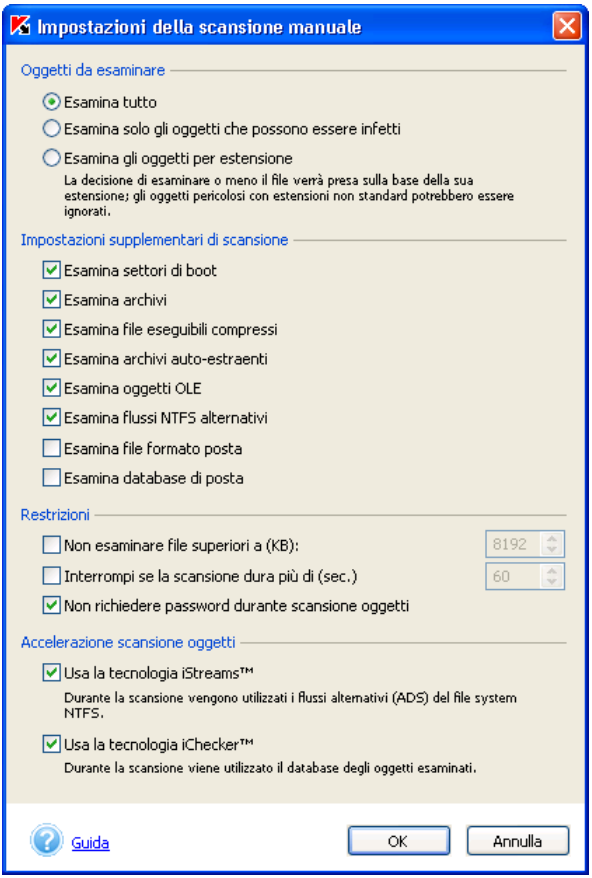
Impostazioni della scansione manuale
Oggetti da esaminare
Esamina tutto
Esamina solo gli oggetti che possono essere infetti
Esamina gli oggetti per estensione
La decisione di esaminare o meno il file verrà presa sulla base della sua estensione; gli oggetti pericolosi con estensioni non standard potrebbero essere ignorati.
Impostazioni supplementari di scansione
Esamina settori di boot
Esamina archivi
Esamina file eseguibili compressi
Esamina archivi auto-estraenti
Esamina oggetti OLE
Esamina flussi NTFS alternativi
Esamina file formato posta
Esamina database di posta
Restrizioni
Non esaminare file superiori a (KB):
8192
Interrompi se la scansione dura più di (sec.)
60
Non richiedere password durante scansione oggetti
Accelerazione scansione oggetti
Usa la tecnologia iStreams™
Durante la scansione vengono utilizzati i flussi alternativi (ADS) del file system NTFS.
Usa la tecnologia iChecker™
Durante la scansione viene utilizzato il database degli oggetti esaminati.
Guida
OK
Annulla

Figura 31. Rifinitura di una scansione manuale

Selezionare le seguenti caselle nella sezione **Restrizioni**:

- **Non esaminare file superiori a (KB):**; specificare le dimensioni massime dell'oggetto da esaminare (in KB) per limitarle ad un certo valore.
- **Interrompi se la scansione dura più di (sec.)**; specificare l'intervallo di scansione in secondi per limitarlo ad un certo valore.
- **Non richiedere password durante scansione oggetti**; disabilita la richiesta della password durante la scansione degli oggetti. Se questa casella è selezionata, gli oggetti protetti da password verranno ignorati durante la scansione.

La sezione **Accelerazione scansione oggetti** consente di abilitare/disabilitare l'utilizzo delle tecnologie di accelerazione della scansione antivirus - iChecker™ e iStreams™. Per fare ciò, selezionare le caselle corrispondenti.

5.3.3.2. Azioni da eseguire su un oggetto rilevato

La sezione **Azioni da eseguire sugli oggetti rilevati** (vedere la Figura 30) consente di selezionare il tipo di azione da eseguire al rilevamento di uno di questi oggetti:

- **Richiedi intervento utente al termine della scansione** – suggerisce di elaborare gli oggetti pericolosi una volta terminata la scansione. Questa modalità è selezionata per impostazione predefinita, poiché non richiede la presenza dell'utente durante la scansione. Poiché la scansione può richiedere molto tempo, è consigliabile utilizzare questa modalità quando non è possibile controllare l'elaborazione degli oggetti pericolosi man mano che vengono rilevati.
- **Richiedi intervento utente durante la scansione** - determina la visualizzazione delle azioni da eseguire sugli oggetti durante la scansione stessa. Viene inoltre visualizzato un elenco di tutte le possibili azioni che possono essere eseguite sull'oggetto, una delle quali figura come raccomandata dagli esperti di Kaspersky Lab. Se non si prevede di abbandonare il computer durante la scansione, si consiglia di selezionare questa modalità di funzionamento.
- **Esegui azione raccomandata** – esegue l'azione raccomandata dagli esperti di Kaspersky Lab. L'azione raccomandata è sempre ben giustificata, di conseguenza è possibile selezionare questa modalità in gran parte dei casi. Sono raccomandate le seguenti azioni:
    - *Disinfetta l'oggetto infetto.*

- Metti in *Quarantena* l'oggetto potenzialmente infetto da virus o una sua modifica.

A volte, dopo aver messo un file in quarantena, può venire visualizzato un messaggio che comunica l'impossibilità di eliminare l'oggetto. Ciò ha a che vedere col fatto che mettere un oggetto in quarantena implica il suo spostamento: viene copiato in quarantena ed eliminato dalla posizione originale. Tuttavia, alcuni oggetti non possono essere cancellati quando vengono spostati, ad esempio se sono attualmente utilizzati da un'altra applicazione.

- *Elimina oggetti infetti* che non è stato possibile o non è possibile disinfettare.

- **Elimina oggetti** - vengono eliminati gli oggetti pericolosi rilevati durante la scansione, senza cercare di disinfettarli e senza richiedere conferma all'utente. Quando un oggetto viene eliminato, ne viene salvata una copia nella memoria di backup. Si consiglia di selezionare questa modalità di funzionamento di Kaspersky Anti-Virus solo se si è sicuri che non si perderanno informazioni importanti.

- **Solo report** - non viene eseguita alcuna azione sull'oggetto interessato. Il programma si limita a registrare l'infezione nell'apposito report. Si consiglia di selezionare questa modalità di funzionamento in casi molto rari, poiché in questo caso gli oggetti pericolosi e nocivi resteranno nel computer.

Ci sono situazioni in cui è impossibile eseguire un'azione sull'oggetto. Ad esempio, quando un oggetto infetto è utilizzato da un'altra applicazione nel momento in cui deve essere esaminato, non può essere elaborato. In tal caso verrà visualizzato un messaggio corrispondente (vedere la Figura 32), che offrirà la possibilità di eseguire una delle seguenti azioni:

- *Disinfettare all'avvio del sistema.* Questa azione verrà elencata solo se l'oggetto può essere disinfettato.

- *Eliminare all'avvio del sistema.*

- *Ignora* - non viene eseguita alcuna azione sull'oggetto interessato. Il programma si limita a registrarne il rilevamento nell'apposito report.

Kaspersky Anti-Virus for Windows Workstations
Attenzione! La disinfezione è impossibile.
Oggetto C:\...\LockFile\eicar.com.cure non può essere disinfettato perché occorre l'autorizzazione per accedere all'oggetto. Si consiglia di disinfettare l'oggetto all'avvio del sistema.
Disinfettare all'avvio del sistema (raccomandato)
Eliminare all'avvio del sistema
Ignora
Applica a tutti oggetti che sono stati bloccati in questa sessione
Guida
Audio OFF
OK

Figura 32. La disinfezione immediata dell'oggetto è impossibile

5.3.4. Scansione di archivi

Kaspersky Anti-Virus esamina gli archivi se è stato selezionato il livello **Protezione massima** o quello **Raccomandato** come livello di protezione, e se la scansione degli archivi non è stata disabilitata (vale a dire, se la casella **Esamina archivi** nella finestra **Impostazioni della scansione manuale** non è stata deselezionata), vedere la Figura 31.

Kaspersky Anti-Virus esamina tutti gli oggetti all'interno dell'archivio, ma disinfetta solo gli oggetti negli archivi zip, arj, cab, rar, lha e ice.
Kaspersky Anti-Virus NON DISINFETTA gli archivi autoestraenti!

Se un archivio o un oggetto all'interno di un archivio è protetto da password ed è abilitata la modalità di richiesta della password, verrà visualizzata una richiesta per la password prima di esaminare tale archivio od oggetto (vedere la Figura 33). Se è stata selezionata la modalità di elaborazione ritardata degli oggetti (vale a dire, se è stata selezionata l'azione **Richiedi intervento utente al termine della scansione** nelle impostazioni, vedere la sezione 5.3.3.2 a pagina 82), verrà visualizzata una richiesta per la password al termine della scansione.

È possibile scegliere se visualizzare o meno la richiesta per la password selezionando o deselezionando la casella **Non richiedere password durante scansione oggetti** nelle impostazioni di scansione (vedere la sezione 5.3.3.1 a pagina 79). Per impostazione predefinita, questa casella è deselezionata solo per il livello di **Protezione massima**.

Kaspersky Anti-Virus for Windows Workstations
Attenzione! L'oggetto è protetto da password.
Per esaminare l'archivio C:\...\eicar.rar\eicar.avc digitare la password con cui è stato creato.
Inserire la password:
Applica a tutti gli oggetti protetti da password in questa sessione
Guida
OK
Ignora
Ignora archivio

Figura 33. Immissione della password per esaminare un archivio

Nel campo **Password**, inserire la password da utilizzare per accedere al file archivio e fare clic su **OK**. Dopo l'inserimento della password, l'applicazione continua ad esaminare l'archivio e gli oggetti in esso contenuti.

Durante l'elaborazione (disinfezione, eliminazione) all'interno di archivi, Kaspersky Anti-Virus decomprime l'archivio che sta elaborando in una cartella temporanea, ne esamina gli oggetti, li elabora, li ri-comprime con lo stesso nome e li ricopia nella posizione originale, sostituendo l'archivio originale esistente. La stessa procedura di elaborazione viene utilizzata per elaborare gli oggetti protetti da password contenuti nell'archivio. La differenza è che, dopo l'elaborazione, gli oggetti verranno compressi nell'archivio senza utilizzare la password.

Per esaminare un altro archivio protetto da password, Kaspersky Anti-Virus applica automaticamente la password dell'archivio precedente a quello successivo da esaminare. Se la password è errata, il programma richiede di inserirne un'altra.

Se non si conosce la password, l'applicazione non sarà in grado di esaminare gli archivi protetti da password. In questo caso è consigliabile fare clic su **Ignora** e proseguire la scansione.

Se un file archivio contiene altri oggetti protetti da password, fare clic sul pulsante **Ignora archivio** per escluderli dalla scansione corrente. Tutti gli altri oggetti non protetti da password all'interno dell'archivio saranno esaminati ed elaborati in base alle impostazioni definite per la scansione antivirus.

La casella **Applica a tutti gli oggetti protetti da password in questa sessione** si applica all'azione selezionata dopo aver selezionato la casella stessa.

Ad esempio, se è stata selezionata questa casella e quindi l'azione **Ignora**, **Ignora archivio**, i rimanenti oggetti protetti da password non saranno esaminati.

Oppure, se si digita la password e si fa clic su OK, l'applicazione tenterà di utilizzare quella password per tutti i rimanenti oggetti protetti da password senza visualizzare altre finestre di dialogo.

Se è impossibile disinfettare l'archivio ed è stata selezionata l'azione **Esegui azione raccomandata** quale azione da eseguire al rilevamento di un oggetto pericoloso, Kaspersky Anti-Virus non eliminerà l'archivio e procederà solo all'inclusione delle informazioni relative al suo rilevamento nel report.

Se è stata selezionata l'azione **Richiedi intervento utente al termine della scansione** o **Richiedi intervento utente durante la scansione** (vedere la sezione 5.3.3.2 a pagina 82) quale azione da eseguire nelle impostazioni di scansione, è possibile eliminare l'archivio che non può essere disinfettato selezionando l'azione **Elimina** nella finestra di dialogo di richiesta. In alternativa, è possibile eliminare questo archivio manualmente.

5.3.5. Scansione delle unità rimovibili

È possibile avviare una scansione delle unità rimovibili dalla finestra principale di Kaspersky Anti-Virus o dal menu di scelta rapida che può essere aperto, ad esempio, dalla finestra di **Esplora risorse** o dal **Desktop**, ecc.

Per esaminare le unità rimovibili dal menu di scelta rapida di Windows,

selezionare le unità (è possibile selezionare l'unità CD e quella floppy contemporaneamente), fare clic col tasto destro del mouse per aprire il menu di scelta rapida di Windows, e selezionare **Scansione antivirus** dal menu (vedere la Figura 27).

Per eseguire la scansione antivirus di un CD o un disco floppy dalla finestra principale dell'applicazione di Kaspersky Anti-Virus,

1. Inserire il CD o il disco floppy nell'unità corrispondente. Si noti che il programma è in grado di esaminare sia il CD che il disco floppy contemporaneamente.
2. Seguire il collegamento Esamina le unità rimovibili nella sezione sinistra della scheda **Protezione** (vedere la figura 2). Questo collegamento viene visualizzato se la casella **Visualizza attività nella scheda "Protezione"** nella sezione informativa dell'attività è stata selezionata (vedere la Figura 28).

oppure

Seguire il collegamento Esamina oggetti per passare alla finestra **Seleziona oggetti da esaminare** (vedere la Figura 26), selezionare le unità rimovibili e scegliere il pulsante **Scansione**.

oppure

Selezionare la scheda **Impostazioni** nella finestra principale dell'applicazione e seguire il collegamento Attività di scansione manuale. Si aprirà la finestra **Attività di scansione manuale** (vedere la Figura 28). Selezionare l'attività **Esamina le unità rimovibili** dall'elenco e scegliere il pulsante **Esegui**.

Subito dopo aver lanciato la scansione, si aprirà una finestra **Scansione in corso...** (vedere la Figura 5) che visualizza l'avanzamento dell'attività mentre viene eseguita con gli oggetti selezionati dall'elenco.

Se è stata selezionata solo un'unità rimovibile per la scansione, una volta terminata la scansione, Kaspersky Anti-Virus suggerirà di inserire il disco successivo.

Si presti attenzione ad alcune particolarità del programma.

- Se si è dimenticato di inserire un CD o un disco floppy prima di avviare la scansione, oppure se la corrispondente periferica rimovibile, unità o unità CD-ROM è scollegata, la scansione non verrà eseguita e l'applicazione non visualizzerà alcun messaggio supplementare per notificarlo.
- Se il disco floppy è stato inserito nell'unità dopo aver avviato la scansione, la scansione non sarà eseguita. Ciò vale anche per i CD-ROM ed altre unità rimovibili.
- Dopo aver rimosso il disco floppy dall'unità o scollegato la periferica rimovibile mentre la scansione era in corso, l'applicazione registrerà un messaggio di errore ma non visualizzerà alcun messaggio supplementare. L'applicazione procederà alla scansione della prossima unità rimovibile (se presente).

Quando viene collegata una nuova unità rimovibile al sistema (vale a dire, quando l'unità viene rilevata dal sistema come nuovo hardware), Kaspersky Anti-Virus esaminerà tale unità alla ricerca di virus di boot, sempre che la protezione in tempo reale sia abilitata.

5.4. Elaborazione degli oggetti nocivi rilevati

La procedura utilizzata da Kaspersky Anti-Virus per elaborare gli oggetti pericolosi, i software nocivi e gli oggetti possibilmente infetti con virus o loro modifiche, una volta rilevati, dipende completamente dalla configurazione della protezione in tempo reale e dalle impostazioni della scansione manuale. Questa

sezione esamina i casi in cui Kaspersky Anti-Virus propone l'esecuzione di varie azioni sugli oggetti rilevati durante la scansione oppure al termine della stessa.

Tale situazioni si verificano quando è stata selezionata una delle seguenti azioni da eseguire sugli oggetti rilevati:

- nelle impostazioni della protezione in tempo reale (vedere la sezione 5.2.1.2 a pagina 58): **Richiedi intervento utente**. In questo caso l'applicazione richiederà l'intervento dell'utente subito dopo il rilevamento di un oggetto pericoloso.
- nelle impostazioni della scansione manuale (vedere la sezione 5.3.3.2 a pagina 82):
    - **Richiedi intervento utente durante la scansione**. Kaspersky Anti-Virus propone all'utente la scelta delle azioni nel momento in cui un tale oggetto viene rilevato.

  oppure

    - **Richiedi intervento utente al termine della scansione** Kaspersky Anti-Virus propone all'utente la scelta dell'azione da eseguire con gli oggetti pericolosi solo se l'elaborazione di tali oggetti è stata avviata, vale a dire, se è stato scelto il pulsante Elabora... nella finestra contenente i risultati della scansione (vedere la Figura 34).

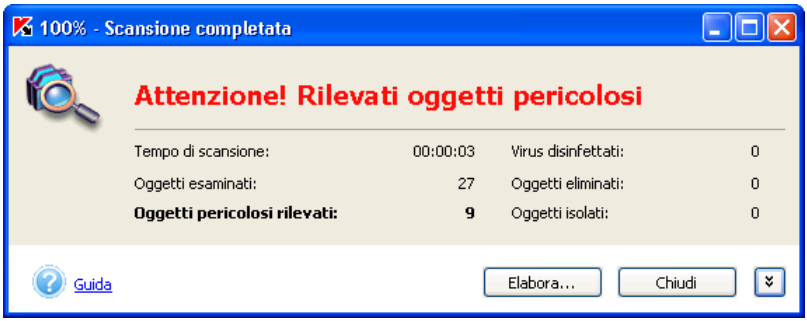

Figura 34. Elaborazione ritardata degli oggetti

Quindi, al rilevamento di un oggetto pericoloso verrà visualizzato un messaggio contenente quanto segue (vedere la Figura 35):

- una descrizione dettagliata dell'oggetto con l'indicazione del nome del malware rilevato;
- un insieme di azioni che possono essere eseguite sull'oggetto. L'elenco delle azioni suggerite contiene sempre un'azione raccomandata dagli esperti di Kaspersky Lab per l'elaborazione dell'oggetto. Accanto ad essa

è visibile la dicitura **(raccomandato)**. Verrà proposta l'esecuzione di una delle seguenti azioni (l'insieme di azioni suggerite dipende dal tipo di oggetto rilevato):

- **Disinfetta** - tenta di disinfettare l'oggetto infetto, se possibile. Prima del primo tentativo di disinfettare l'oggetto, ne verrà salvata una copia nella memoria di backup.
- **Elimina** - elimina l'oggetto infetto o possibilmente infetto. Quando un oggetto viene eliminato, ne viene salvata una copia nella memoria di backup.
- **Ignora** - non viene eseguita alcuna azione sull'oggetto. Il programma si limita a registrarne il rilevamento nel report.
- **Quarantena** - l'oggetto possibilmente infetto da virus o da una sua modifica viene spostato in quarantena per poi esaminarlo, ripristinarlo, inviarlo a Kaspersky Lab per l'analisi o eliminarlo.
- **Ignora, aggiungi a esclusioni** - il programma rilevato viene aggiunto all'elenco di esclusioni dalla definizione della scansione antivirus e della protezione.

Per utilizzare le esclusioni aggiunte, selezionare la casella **Escludi riskware consentito** nella finestra **Elenco esclusioni** (vedere la figura 38).

Kaspersky Anti-Virus for Windows Workstations
Attenzione! Rilevato oggetto infetto.
Oggetto C:\...\Eicar.zip\Eicar.com è infetto da virus EICAR-Test-File. Si consiglia di disinfettare l'oggetto.
Disinfetta (raccomandato)
Elimina
Ignora
Applica a tutti infetti oggetti, che possono essere disinfettati (in questa sessione)
Guida
Audio OFF
OK

Figura 35. Notifica del rilevamento di un oggetto infetto

È inoltre possibile applicare l'azione selezionata a tutti gli oggetti di questo tipo selezionando la casella corrispondente. Quindi, ad esempio, per applicare l'azione selezionata a tutti gli oggetti infetti che possono essere disinfettati

dall'applicazione, selezionare la casella **Applica a tutti i casi di infezione di oggetti, che possono essere disinfettati (in questa sessione)**.

Se, per qualsiasi ragione, si è deciso di non elaborare gli oggetti selezionando l'opzione **Ignora**, è possibile elaborarli in seguito. Per fare ciò, seguire il collegamento trattare questi oggetti nella sezione destra della scheda **Protezione**. Si aprirà la finestra di dialogo **Oggetti pericolosi rilevati** (vedere la Figura 36) che contiene una descrizione dettagliata di ciascun oggetto pericoloso nonché il collegamento alla descrizione corrispondente nell'enciclopedia dei virus, all'indirizzo www.viruslist.com.

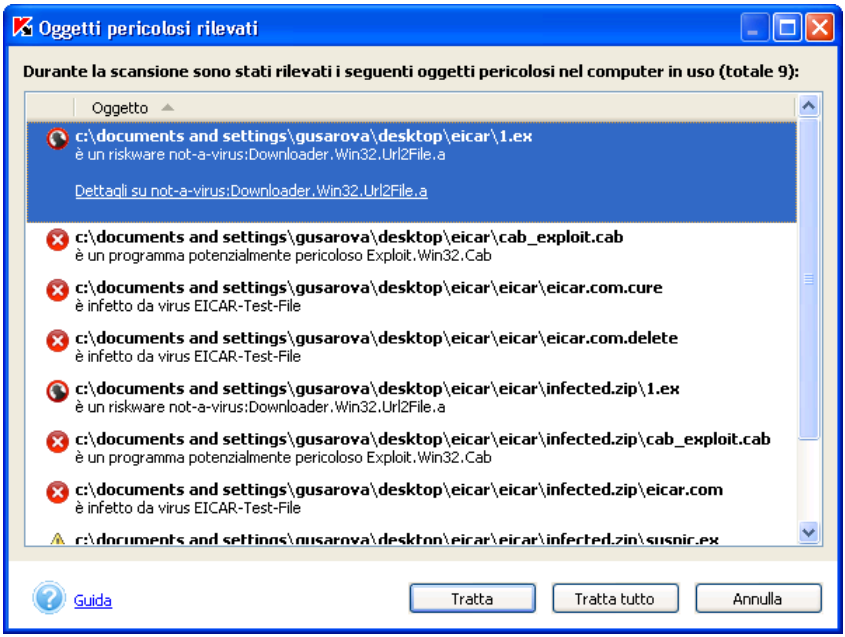

Figura 36. Elenco degli oggetti pericolosi rilevati

È possibile elaborare l'oggetto selezionato dall'elenco scegliendo il pulsante **Tratta**, oppure avviare l'elaborazione di tutti gli oggetti nell'elenco scegliendo il pulsante **Tratta tutto**. L'applicazione visualizzerà allora dei messaggi (vedere la Figura 35) che possono essere utilizzati per selezionare un'azione da eseguire sull'oggetto (per una descrizione dettagliata delle azioni possibili, vedere sopra).

Per eliminare un oggetto dall'elenco senza elaborarlo, scegliere il comando **Elimina dall'elenco** dal menu di scelta rapida (vedere la Figura 37).

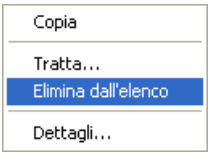

Figura 37. Menu di scelta rapida della finestra di dialogo **Oggetti pericolosi rilevati**

Se uno qualsiasi degli oggetti pericolosi è stato eliminato manualmente, verrà rimosso dall'elenco nel momento in cui si cercherà di disinfettarlo.

5.5. Monitoraggio dei processi software

Kaspersky Anti-Virus consente di creare un elenco di processi software che non saranno monitorati dall'applicazione antivirus.

Ad esempio, si considerano sicuri tutti gli oggetti utilizzati dal **Blocco note**, un'applicazione standard di Microsoft Windows, e non si ritiene necessario che tali oggetti vengano esaminati nella modalità di protezione in tempo reale. In altre parole, si considerano affidabili i processi di quest'applicazione. Per escludere gli oggetti utilizzati da questo processo dalla definizione della scansione per la protezione in tempo reale, aggiungere l'applicazione **Blocco note** all'elenco di processi affidabili.

Per creare un elenco di processi affidabili,

scegliere il collegamento specificato/non specificato accanto all'impostazione **processi attendibili** nella sezione **Impostazione di protezione** della scheda **File** (vedere la Figura 16).

Ciò aprirà la finestra **Elenco esclusioni** (vedere la figura 38). Per aggiungere nuovi processi a questo elenco o modificarlo, utilizzare i pulsanti a destra dell'elenco.

Scegliendo il pulsante **Aggiungi...**, è possibile aggiungere i seguenti oggetti all'elenco esclusioni:

- un file eseguibile. Per fare ciò, scegliere il pulsante **Sfoglia** e specificare un file con estensione **.exe**;

- *processi in esecuzione.* Per fare ciò, scegliere il comando **Processi in esecuzione** e selezionare uno dei processi nell'elenco a discesa.

Per eliminare il processo dall'elenco, specificare il processo desiderato e scegliere il pulsante **Elimina**.

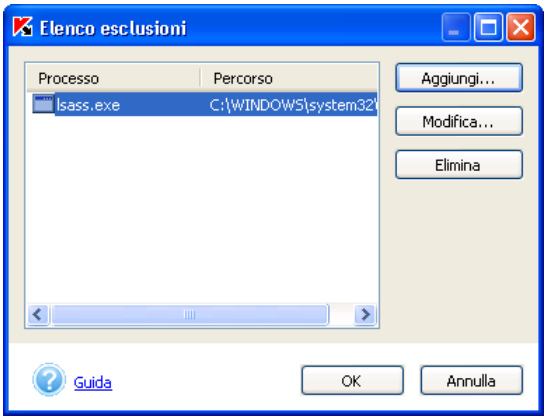

Figura 38. Finestra dell'elenco dei processi attendibili

Si aprirà un ulteriore finestra quando si sceglie il pulsante **Modifica...** (vedere la Figura 39).

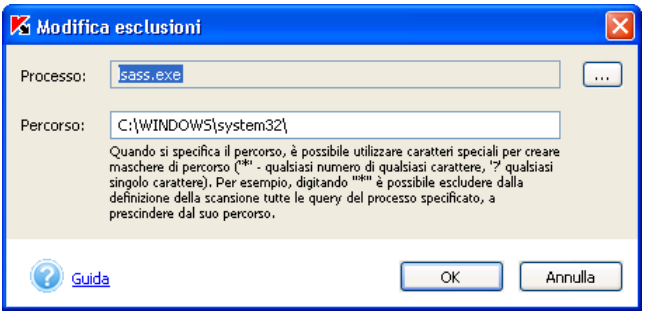
Modifica esclusioni
Processo:
lsass.exe
...
Percorso:
C:\WINDOWS\system32\
Quando si specifica il percorso, è possibile utilizzare caratteri speciali per creare maschere di percorso ('*' - qualsiasi numero di qualsiasi carattere, '?' qualsiasi singolo carattere). Per esempio, digitando "*" è possibile escludere dalla definizione della scansione tutte le query del processo specificato, a prescindere dal suo percorso.
Guida
OK
Annulla

Figura 39. Aggiunta di un processo attendibile

Il nome del file del processo può essere selezionato scegliendo il pulsante . Quando si seleziona un nome, Kaspersky Anti-Virus ricorda gli attributi interni dei file del processo che lo identificano come attendibile durante la scansione antivirus.

Il percorso al file verrà fornito automaticamente quando se ne seleziona il nome. È possibile modificarlo manualmente.

Quando si specifica il percorso, utilizzare il percorso completo al file del processo, oppure utilizzare una maschera * (qualsiasi numero di caratteri qualsiasi) o ? (qualsiasi singolo carattere).
Se ad esempio si utilizza la maschera *, il processo in esecuzione sarà considerato affidabile a prescindere dalla cartella in cui si trova il file del processo.

Se si desidera escludere i programmi consentiti dalla definizione della scansione, selezionare la casella **Escludi riskware consentito** nella finestra **Elenco esclusioni** (vedere la figura 38). Questi programmi sono elencati nella finestra **Codici ostili ed esclusioni** che si apre scegliendo il pulsante **Dettagli...** (vedere la sezione 5.7 a pagina 94).

5.6. Attività utente

Durante l'installazione di Kaspersky Anti-Virus viene generato un elenco di attività di sistema. Esso comprende sia attività di aggiornamento (aggiornamento dei database antivirus o dei moduli dell'applicazione, ripristino della versione precedente del database) che di scansione (scansione delle risorse del computer, delle unità rimovibili e della quarantena, scansione automatica all'avvio dell'applicazione).

È possibile lanciare le attività di sistema per impostazione predefinita, configurarne i parametri e pianificarle. Queste attività non possono essere eliminate.

Il processo di impostazione dei parametri per le attività di aggiornamento del database e dei componenti dell'applicazione è descritto nella sezione 5.1 a pagina 39. L'attività di ripristino della versione precedente del database non prevede impostazioni specifiche.

Lavorando con Kaspersky Anti-Virus, gli amministratori possono creare e gestire attività di scansione di oggetti personalizzati.

Gli utenti delle workstation non hanno accesso alla creazione e all'impostazione delle attività. Essi possono visualizzare un elenco delle attività create dall'amministratore nel riquadro sinistro della scheda **Protezione** (vedere la Figura 2), ed eseguirle.

Se si utilizza l'amministrazione remota di Kaspersky Anti-Virus, l'elenco di attività includerà anche quelle locali e di gruppo create tramite Kaspersky Administration Kit (vedere la sezione 6.2 a pagina 155). La gestione delle attività locali è analoga alla gestione delle attività create dall'utente: è possibile lanciarle, eliminarle e modificarne le impostazioni. Le attività di gruppo non possono essere lanciate od eliminate, né è possibile modificarne le impostazioni; la gestione di tali attività è possibile esclusivamente tramite Kaspersky Administration Kit.

Se la modifica di determinate impostazioni è stata proibita durante la gestione delle attività tramite Kaspersky Administration Kit (è stato impostato un blocco), non sarà possibile modificare tali attività tramite l'interfaccia locale di Kaspersky Anti-Virus.

Per creare una nuova attività,

scegliere il pulsante **Crea** nella finestra **Attività di scansione manuale** (vedere la Figura 28). Si aprirà una finestra (vedere la Figura 29) contenente le seguenti schede: **Oggetti da esaminare**, **Impostazioni**, **Pianifica** e **Esegui per conto dell'account utente**.

Immettere il nome dell'attività nel campo **Nome attività** e configurare tutte le altre impostazioni (per dettagli, vedere la sezione 5.3.3 a pagina 76).

Il riquadro relativo a ciascuna attività contiene la casella **Visualizza attività nella scheda "Protezione"** che ne controlla la visualizzazione nella finestra principale dell'applicazione. Se la casella è selezionata, gli utenti della workstation potranno vedere l'attività nella parte sinistra della scheda e potranno lanciarla.

Per eliminare un'attività dall'elenco, selezionarla e scegliere il pulsante **Elimina**. Tuttavia, si tenga presente che è possibile eliminare dall'elenco solo le attività aggiunte manualmente. Le attività di sistema e di gruppo create tramite Kaspersky Administration Kit non possono essere eliminate.

Per lanciare un'attività, selezionarla dall'elenco e scegliere il pulsante **Esegui**. Si aprirà una finestra contenente informazioni sull'avanzamento dell'esecuzione dell'attività.

Per visualizzare le impostazioni dell'attività creata, selezionarla dall'elenco e scegliere il pulsante **Proprietà...**.

5.7. Creazione di un elenco di esclusioni

Alcune situazioni richiedono l'esclusione di alcuni oggetti dall'ambito di scansione o protezione antivirus. Tali elenchi di esclusioni vengono creati per le attività di scansione manuale e di protezione file e posta in tempo reale.

L'elenco generale di tutte le esclusioni dalla protezione antivirus del computer può essere visualizzato e modificato dalla finestra speciale **Codici ostili ed esclusioni** (vedere la Figura 14). Per aprire questa finestra, seguire il collegamento Codici ostili ed esclusioni scansione nella sezione sinistra della scheda **Impostazioni** (vedere la figura 3). L'elenco di esclusioni viene creato utilizzando i pulsanti corrispondenti.

Per aggiungere un'esclusione, scegliere il pulsante ***Aggiungi...****.*

Si aprirà la finestra **Oggetto da escludere** (vedere la Figura 40) che consente di specificare le esclusioni per Kaspersky Anti-Virus.

È possibile specificare come esclusioni i seguenti tipi di oggetti:

- *Dischi, cartelle, file, maschere di file*.
- *Codici ostili* - diversi tipi di programmi nocivi e a rischio;
- *File legati a codici ostili specifici* - file specifici ai quali sono stati assegnati certi tipi di codici ostili dopo la scansione.

Per escludere una certa cartella o un certo file (utilizzando una maschera) dall'ambito della protezione di Kaspersky Anti-Virus,

compilare il campo **Oggetto** utilizzando il pulsante ....

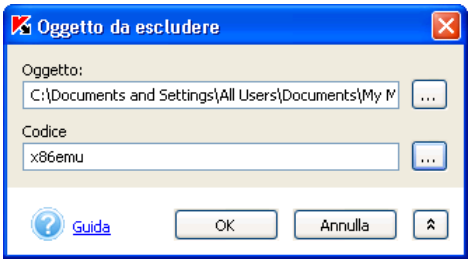

Figura 40. Creazione di un elenco di esclusioni

Quando si crea un percorso alla cartella o all'oggetto che si desidera escludere dall'ambito di scansione, è possibile utilizzare le variabili di ambiente del sistema. Ad esempio, è possibile escludere la cartella di installazione di Windows dall'ambito di scansione specificando la variabile **%windir%**.

Quando si aggiungono oggetti utilizzando maschere, è possibile immettere diverse maschere contemporaneamente, separandole con uno spazio. Se il nome di un file contiene spazi, tale nome deve essere immesso tra virgolette.

Di seguito sono riportati esempi di maschere di esclusione consentite:

- Maschere senza percorso agli oggetti:
  - ***.exe** - tutti i file con estensione *exe*

- ***.ex?** - tutti i file con estensione *ex?*, dove ? rappresenta qualsiasi singolo carattere
- **test** - tutti i file il cui nome è *test*

- Maschere con percorsi assoluti agli oggetti:
  - **C:\dir*.*** - tutti i file contenuti nella cartella *C:\dir*
  - **C:\dir*.exe** - tutti i file con estensione exe nella cartella *C:\dir*
  - **C:\dir*.ex? -** tutti i file con estensione *ex?* nella cartella *C:\dir*, dove ? rappresenta qualsiasi singolo carattere
  - **C:\dir\test** - solo il file *C:\dir\test*
  - **C:\dir** - tutti i file contenuti nella cartella *C:\dir* e nelle relative sottocartelle.
- Maschere con percorsi relativi agli oggetti:
  - **dir*.*** - tutti i file contenuti in tutte le cartelle di nome *dir*
  - **dir\test** - tutti i file di nome test nelle cartelle di nome *dir*
  - **dir*.exe** - tutti i file con estensione *exe* in tutte le cartelle di nome *dir*
  - **dir*.ex?** - tutti i file con estensione *ex?* in tutte le cartelle *dir*, dove ? rappresenta qualsiasi singolo carattere
  - **dir** - tutti i file in tutte le cartelle di nome *dir* e in tutte le sottocartelle di tali cartelle

È sconsigliabile specificare esclusioni immettendo la maschera *.* o *, poiché ciò equivale a disattivare completamente la protezione in tempo reale.

È sconsigliabile specificare come esclusione qualsiasi disco virtuale creato sulla base della cartella del file system utilizzando il comando *subst*. Ciò e privo di significato, poiché durante la scansione Kaspersky Anti-Virus tratta questo disco virtuale come cartella e quindi lo esamina.

Per escludere dall'ambito dell'elaborazione antivirus tutti i file ai quali è stato assegnato un certo tipo di codice ostile in conseguenza della scansione,

aprire la parte addizionale della finestra (vedere la Figura 40) scegliendo il pulsante e selezionare un codice ostile nella finestra **Elenco delle minacce rilevate** (vedere la Figura 41), che si apre scegliendo il pulsante .

Questa finestra consente di ricercare un codice ostile specifico utilizzando una parte del suo nome, ordinare l'elenco di codici ostili facendo clic sull'intestazione della colonna **Nome**, e copiare il nome del codice ostile negli appunti tramite il corrispondente comando dal menu di scelta rapida. È possibile accedere ad una dettagliata descrizione dei codici ostili all'indirizzo www.viruslist.com. Per fare ciò, selezionare un codice ostile dall'elenco ed utilizzare il comando **Dettagli** dal menu di scelta rapida.

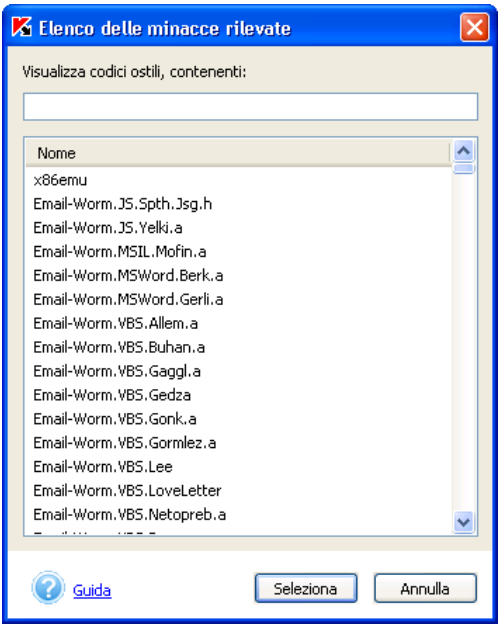

Figura 41. L'elenco delle minacce rilevate

Per escludere un oggetto specifico di un codice ostile conosciuto dall'ambito della protezione,

1. Specificare il nome dell'oggetto nel campo **Oggetto**.
2. Immettere il tipo di codice ostile nel campo **Codice**.

È possibile escludere un file di un certo tipo di codice ostile utilizzando un messaggio di notifica che si apre quando un file di questo tipo viene rilevato da Kaspersky Anti-Virus (vedere la Figura 42). Se si ritiene che questo programma non sia pericoloso e possa essere utilizzato nel computer, selezionare l'opzione **Ignora, aggiungi a esclusioni**. Il programma verrà aggiunto all'elenco di esclusioni dall'ambito di scansione nella finestra **Codici ostili ed esclusioni** (vedere la Figura 14).

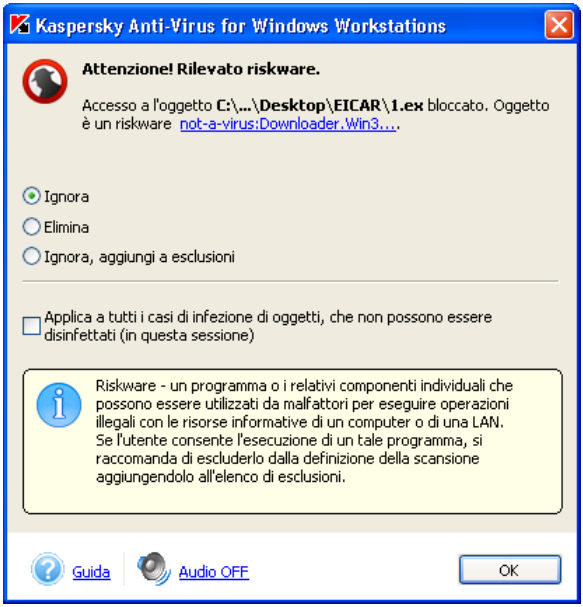
Kaspersky Anti-Virus for Windows Workstations
Attenzione! Rilevato riskware.
Accesso a l'oggetto C:\...\Desktop\EICAR\1.ex bloccato. Oggetto è un riskware not-a-virus:Downloader.Win3....
Ignora
Elimina
Ignora, aggiungi a esclusioni
Applica a tutti i casi di infezione di oggetti, che non possono essere disinfettati (in questa sessione)
Riskware - un programma o i relativi componenti individuali che possono essere utilizzati da malfattori per eseguire operazioni illegali con le risorse informative di un computer o di una LAN. Se l'utente consente l'esecuzione di un tale programma, si raccomanda di escluderlo dalla definizione della scansione aggiungendolo all'elenco di esclusioni.
Guida
Audio OFF
OK

Figura 42. Notifica relativa ad un codice ostile

5.8. Pianificazione

È possibile pianificare il lancio automatico delle attività di scansione manuale o aggiornamento. Ciò consentirà di aggiornare puntualmente il database antivirus e di eseguire regolarmente una scansione antivirus degli oggetti nel computer, in base a tale database aggiornato.

Per impostazione predefinita, Kaspersky Anti-Virus aggiorna il database antivirus ogni tre ore ed esegue una scansione completa del computer ogni venerdì alle 20:00.

Per modificare il piano di aggiornamento del database antivirus,

1. utilizzare il collegamento Configura aggiornamento nella sezione sinistra della scheda **Impostazioni**.
2. Nella finestra che si aprirà, selezionare l'attività per la quale si desidera creare/modificare un piano e scegliere il pulsante **Proprietà**.

Si aprirà la finestra delle impostazioni di 'aggiornamento nella scheda **Pianifica** (vedere la Figura 8).

Per creare/modificare un piano per l'attività di scansione manuale,

1. utilizzare il collegamento Attività di scansione manuale nella sezione sinistra della scheda **Impostazioni**.
2. Nella finestra contenente l'elenco di attività di scansione (vedere la Figura 28), selezionare l'attività per la quale si desidera creare/modificare il piano e scegliere il pulsante **Proprietà**.

Si aprirà una finestra di rifinitura per questa attività (vedere la Figura 29). Per configurare il piano, passare alla scheda **Pianifica** (vedere la Figura 43).

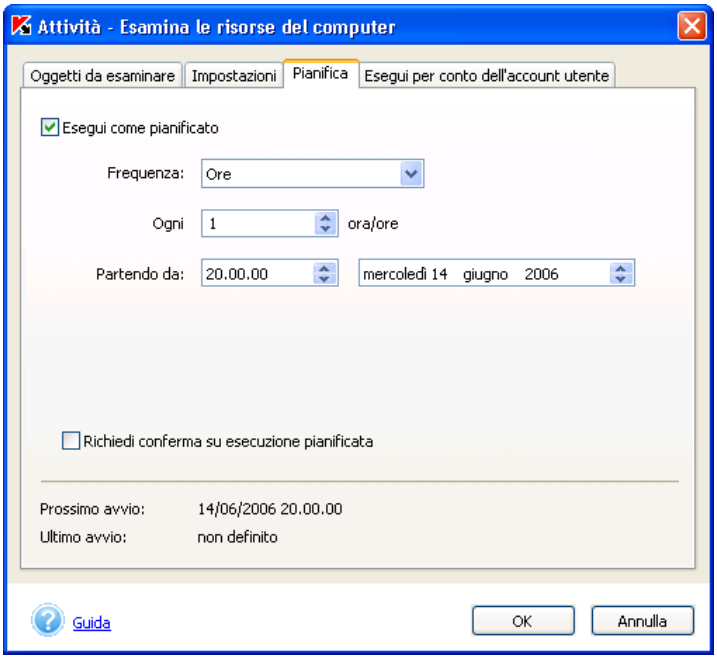

Figura 43. Creazione di una nuova attività. La scheda **Pianifica**

Per abilitare il lancio automatico dell'attività pianificata, selezionare la casella **Esegui come pianificato**.

Se si desidera ricevere notifiche circa gli aggiornamenti che stanno per essere eseguiti, selezionare la casella **Richiedi conferma su esecuzione pianificata**. Se questa casella è selezionata, sullo schermo verrà visualizzata una finestra

Esecuzione attività pianificata (vedere la Figura 44) prima del lancio dell'attività di scansione pianificata. Scegliere il pulsante **Inizio** per avviare la scansione pianificata. Per ritardare l'esecuzione dell'attività per un certo tempo, selezionare l'intervallo desiderato nell'elenco a discesa e scegliere il pulsante **Ritardo**. Se entro 3 minuti non viene selezionata alcuna azione, l'attività verrà avviata automaticamente.

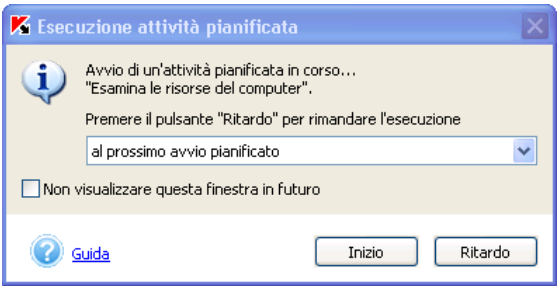

Figura 44. Richiesta di conferma per il lancio di un'attività pianificata

Utilizzare il campo **Frequenza** per definire la periodicità dell'attività. Sono disponibili le seguenti opzioni: *Ore*, *Giorni*, *Settimane, All'avvio del programma*. A seconda dell'opzione selezionata, l'aspetto della parte centrale della finestra, contenente i campi di immissione dati, cambia:

- *Ore* - l'attività sarà eseguita, secondo quanto pianificato, ogni *x* ore. Definire la frequenza (in ore), la data e l'ora a per la prima esecuzione.

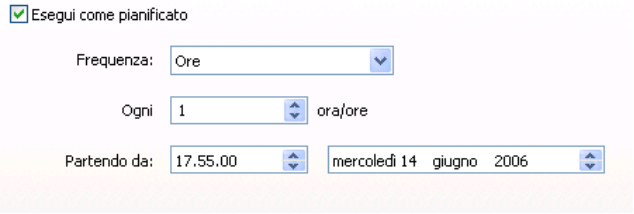

Figura 45. Pianificazione dell'attività con frequenza oraria

- *Giorni* - l'attività sarà eseguita, secondo quanto pianificato, ogni *x* giorni. Definire la frequenza (in giorni) e l'ora per la prima esecuzione.

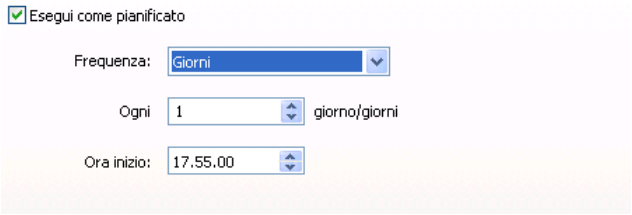

Figura 46. Pianificazione dell'attività con frequenza quotidiana

- *Settimane* - l'attività sarà eseguita, secondo quanto pianificato, ogni *x* settimane. Definire la frequenza (in settimane) e selezionare il giorno della settimana e l'ora d'esecuzione.

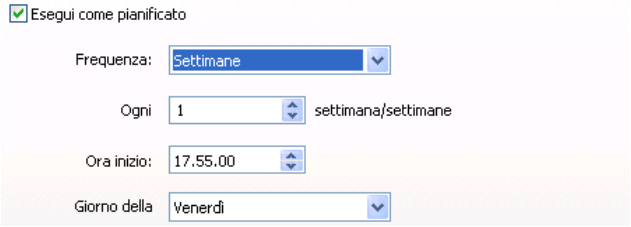

Figura 47. Pianificazione dell'attività con frequenza settimanale

- *All'avvio del programma* L'attività verrà eseguita immediatamente all'avvio di Kaspersky Anti-Virus.

5.9. Lancio di un'attività per conto di un account utente selezionato

Kaspersky Anti-Virus consente di avviare un'attività per conto di un account utente diverso da quello corrente.

Per impostazione predefinita, questo servizio è disabilitato e le attività vengono avviate per conto dell'account corrente. Quando il servizio è abilitato, l'amministratore configura l'account che dispone di diritti sufficienti per l'accesso all'oggetto: per esempio, un'attività di scansione manuale richiede diritti sufficienti ad accedere all'oggetto esaminato, mentre un'attività di aggiornamento richiede il diritto di accedere ad una cartella locale di aggiornamento o i diritti di un utente autorizzato del server proxy.

In questo modo si evitano errori durante l'esecuzione di un'attività di scansione manuale o di aggiornamento, quando l'utente che ha avviato l'attività non dispone dei diritti di accesso richiesti.

È possibile configurare l'avvio di attività antivirus per conto di un altro account utente nella scheda **Esegui per conto dell'account utente** (vedere la 48).

Per abilitare questo servizio, selezionare la casella **Esegui attività per conto dell'account utente.**. Per impostazione predefinita, questa casella è deselezionata e le attività vengono avviate con i diritti dell'account corrente.

Utilizzando il campo sottostante, immettere le informazioni relative all'account per conto del quale verrà avviata l'attività: nome utente e password.

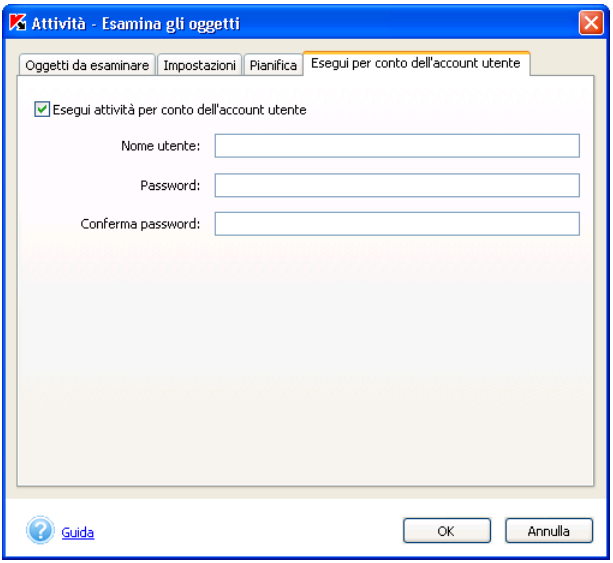

Figura 48. La scheda **Esegui per conto dell'account utente**.

5.10. Funzionalità supplementari

Kaspersky Anti-Virus consente diverse funzionalità supplementari per la personalizzazione e l'uso del prodotto, fra cui:

- Lavorare con oggetti sospetti trasferiti nella cartella della quarantena.
- Lavorare con copie di backup di oggetti eliminati o modificati da Kaspersky Anti-Virus e trasferiti nella memoria di backup.
- Visualizzare il registro di funzionamento dell'applicazione.
- Gestione della configurazione di Kaspersky Anti-Virus
- Impostazioni supplementari.

- Configurare le richieste di conferma
- Funzionamento in modalità amministratore e modalità utente

5.10.1. Cartella della quarantena e memoria di backup

Kaspersky Anti-Virus consente di isolare gli oggetti sospetti in quarantena o di salvare copie degli oggetti infetti nella memoria di backup prima di procedere alla riparazione o all'eliminazione.

Quando rileva un oggetto sospetto, l'applicazione lo isola nella cartella riservata alla quarantena, dove potrà essere riesaminato, eliminato, ripristinato o inviato a Kaspersky Lab per ulteriori analisi.

Prima di cercare di riparare o eliminare un oggetto infetto, l'applicazione ne crea una copia di backup dopo il rilevamento. Questa copia viene salvata nella cartella di backup, dalla quale l'oggetto potrà essere successivamente ripristinato qualora contenga dati importanti.

5.10.1.1. Configurazione dell'archiviazione

Per rivedere o modificare le impostazioni di archiviazione in quarantena o nella memoria di backup,

seguire il collegamento Configura quarantena e backup nel riquadro sinistro della scheda **Impostazioni**.

È possibile definire i parametri di entrambe le cartelle di archiviazione tramite le schede presenti nella finestra **Impostazione della memoria di quarantena e backup**.

In questa finestra (vedere la Figura 49), modificare le seguenti impostazioni per la quarantena e la memoria di backup nelle schede corrispondenti:

- **Elimina oggetti memorizzati da oltre, (giorni):** Per impostazione predefinita, il periodo massimo di archiviazione dei file in quarantena è illimitato (la casella non è selezionata). È possibile limitare il periodo di archiviazione selezionando questa casella e specificando il numero desiderato di giorni nel campo di immissione (per impostazione predefinita, il periodo suggerito è 90 giorni).
- **Dimens. max. (MB):** Per impostazione predefinita, la dimensione massima della quarantena è illimitata (la casella non è selezionata). Se si desidera limitare la dimensione totale massima disponibile per i file in

quarantena, selezionare questa casella ed immettere il valore desiderato per specificare la dimensione massima (il valore predefinito è 100 MB). Selezionare l'azione eseguita da Kaspersky Anti-Virus in caso di sovraccarico dell'archivio:

- *Avvisa utente* - visualizza un messaggio con l'invito a selezionare ulteriori azioni in caso di sovraccarico della quarantena.
- *Rimuovi gli oggetti più vecchi* - elimina i file messi in quarantena prima di tutti gli altri.

Esamina automaticamente oggetti in quarantena ad ogni aggiornamento del database antivirus Questa modalità consente la scansione automatica degli oggetti in quarantena ogniqualvolta il database viene aggiornato, senza alcun intervento da parte dell'utente.

Kaspersky Anti-Virus non è in grado di esaminare gli oggetti in quarantena subito dopo l'aggiornamento del database antivirus se al momento si sta lavorando con la quarantena.

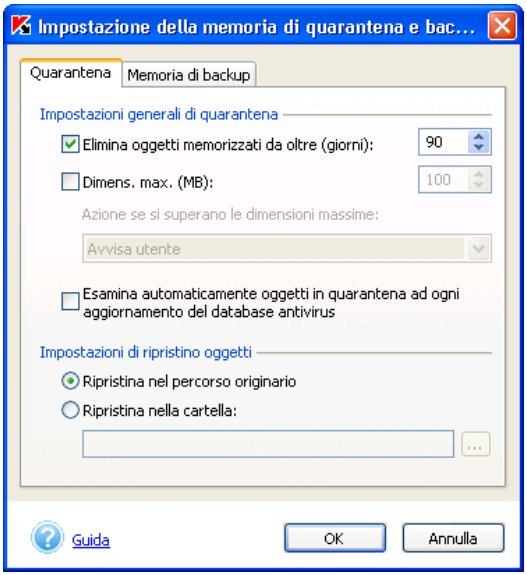

Figura 49. Configurazione delle impostazioni di quarantena

Specificare la posizione in cui gli oggetti saranno ripristinati nella sezione **Impostazioni di ripristino oggetti**:

- **Ripristina nel percorso originario**. Per impostazione predefinita, la copia ripristinata verrà salvata nella posizione in cui Kaspersky Anti-Virus aveva rilevato l'oggetto originale.
- **Ripristina nella cartella**. Se si seleziona questa opzione, specificare il percorso alla cartella nella quale si desidera ripristinare gli oggetti.

Le impostazioni della memoria di backup che definiscono la dimensione massima, il periodo massimo di archiviazione ed il ripristino delle copie di backup sono analoghe alle corrispondenti impostazioni della quarantena.

5.10.1.2. Funzionamento dell'archiviazione in quarantena

Kaspersky Anti-Virus trasferisce tutti gli oggetti sospetti rilevati durante le scansioni complete del computer o in modalità di protezione in tempo reale nella quarantena, dove è possibile riesaminarli, ripristinarli, eliminarli, ecc.

Per impostazione predefinita, Kaspersky Anti-Virus riesamina gli oggetti in quarantena dopo ogni aggiornamento del database antivirus. Se si desidera esaminare manualmente gli oggetti in quarantena, si consiglia di aggiornare prima il database antivirus. I database aggiornati possono già contenere informazioni sui virus sospettati di aver infettato i file, consentendone così la disinfezione.

Le operazioni con i file sospetti vengono eseguite nella finestra **Quarantena** (vedere la Figura 50), che si apre facendo clic sul collegamento Visualizza quarantena nella scheda **Protezione** (vedere la Figura 2) della finestra principale dell'applicazione, oppure sul collegamento Visualizza quarantena nella finestra di scansione (vedere la Figura 5).

La scheda **Protezione** (vedere la figura 2) visualizza il numero totale di oggetti in quarantena tra parentesi, accanto al collegamento Visualizza quarantena.

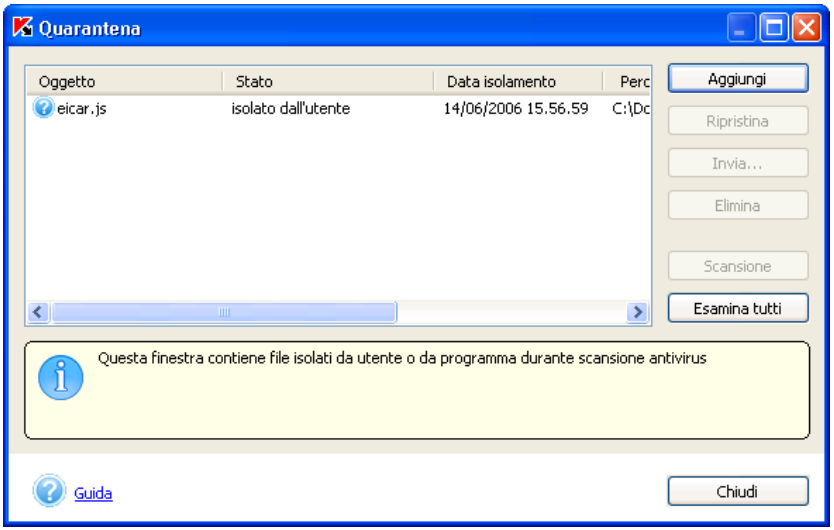

Figura 50. Finestra Quarantena

Questa finestra di dialogo consente di eseguire le seguenti operazioni:

- Mettere in quarantena un file che si sospetta contenere un virus, anche se non è stato rilevato come tale da Kaspersky Anti-Virus. Per fare ciò, scegliere il pulsante **Aggiungi** e selezionare il file sospetto nella finestra standard di selezione file. Questo file verrà aggiunto all'elenco con lo stato *isolato dall'utente*.

- Esaminare e disinfettare tutti i file sospetti o selezionati da un elenco utilizzando il database antivirus corrente. Per fare ciò, scegliere il pulsante **Esamina tutto** o il pulsante **Scansione** (dopo aver selezionato gli oggetti da esaminare).

  La scansione e la disinfezione di qualsiasi oggetto in quarantena può modificarne lo stato in *infetto, probabilmente infetto, falso allarme, non infetto, ecc.*

  Lo stato *infetto* significa che l'oggetto è stato identificato come infetto, ma la sua disinfezione non è riuscita. Si raccomanda di eliminare gli oggetti caratterizzati da questo stato.

  Tutti gli oggetti caratterizzati dallo stato *falso allarme* possono essere ripristinati in tutta sicurezza in quanto il precedente stato *probabilmente infetto* non è stato confermato da Kaspersky Anti-Virus.

È possibile eseguire l'attività **Esamina oggetti in quarantena** della finestra **Attività di scansione manuale** (vedere la Figura 28). Quando viene avviata l'attività, si apre una finestra di **Scansione** (vedere la Figura 5). Il rapporto visualizza risultati della scansione.
L'attività **Esamina oggetti in quarantena** è analoga all'attività avviata tramite il pulsante **Esamina tutto** nella finestra **Quarantena** (vedere la Figura 50).

- Ripristinare i file nelle stesse cartelle dalle quali sono stati spostati in quarantena. Per ripristinare un oggetto, selezionarlo dall'elenco e scegliere il pulsante **Ripristina**. Per ripristinare oggetti che sono stati messi in quarantena da archivi, database di posta e file in formato posta, è inoltre necessario specificare la cartella in cui ripristinarli.

Si raccomanda di ripristinare solo gli oggetti caratterizzati dagli stati falso allarme, non infetto o disinfettato, poiché il ripristino di altri oggetti può causare l'infezione del computer con un virus!

- Inviare i file sospetti agli esperti di Kaspersky Lab per l'analisi. Si raccomanda di inviare un oggetto agli esperti per l'analisi solo nei casi in cui il suo stato di probabile infezione non sia mutato dopo diverse scansioni e vari tentativi di disinfezione. Per inviare il file agli esperti per l'analisi, scegliere il pulsante Invia (per dettagli, vedere la Appendice A a pagina 199).

Si noti che ciascun file inviato a Kaspersky Lab per l'analisi dev'essere esaminato con Kaspersky Anti-Virus utilizzando il database antivirus aggiornato almeno al giorno precedente la data dell'invio.

- Eliminare oggetti o gruppi di oggetti selezionati dalla quarantena. Eliminare solo gli oggetti che non possono essere disinfettati. Per eliminare gli oggetti, selezionarli dall'elenco e scegliere il pulsante **Elimina**.

5.10.1.3. Funzionamento della memoria di backup

Kaspersky Anti-Virus crea una copia di ogni oggetto infetto o sospetto prima di tentarne la disinfezione o l'eliminazione; tale copia viene salvata nella memoria di backup.

Quando necessario, è possibile ripristinare qualsiasi oggetto: se, per esempio, la disinfezione ha causato perdite di dati, se l'oggetto è stato erroneamente

eliminato o se si desidera ritentarne la disinfezione con database antivirus più aggiornati.

Le copie di backup vengono gestite nella finestra **Backup** (vedere la figura 51), che si apre facendo clic sul collegamento Memoria di backup nella scheda **Protezione** (vedere la figura 2) della finestra principale dell'applicazione.

La scheda **Protezione** (vedere la figura 2) visualizza il numero totale di copie di backup di oggetti tra parentesi, accanto al collegamento Memoria di backup.

La finestra Backup consente di eseguire le seguenti operazioni:

- Ripristinare gli oggetti nelle cartelle originarie dalle quali sono stati aggiunti alla memoria di backup, o in cartelle specifiche. Per ripristinare un oggetto, selezionarlo dall'elenco e scegliere il pulsante **Ripristina**.

  L'oggetto verrà ripristinato dalla copia di backup col nome originale che aveva prima del tentativo di disinfezione.

  Se un oggetto con lo stesso nome è già presente nella posizione originale (questa situazione è possibile quando si sta ripristinando un oggetto la cui copia è stata creata prima del tentativo di disinfezione), verrà visualizzato un corrispondente messaggio di notifica. È possibile modificare la posizione di ripristino dell'oggetto o rinominarlo.

- Eliminare file o gruppi di file selezionati dalla memoria di backup. Per eliminare un file, selezionarlo dall'elenco e scegliere il pulsante **Elimina**.

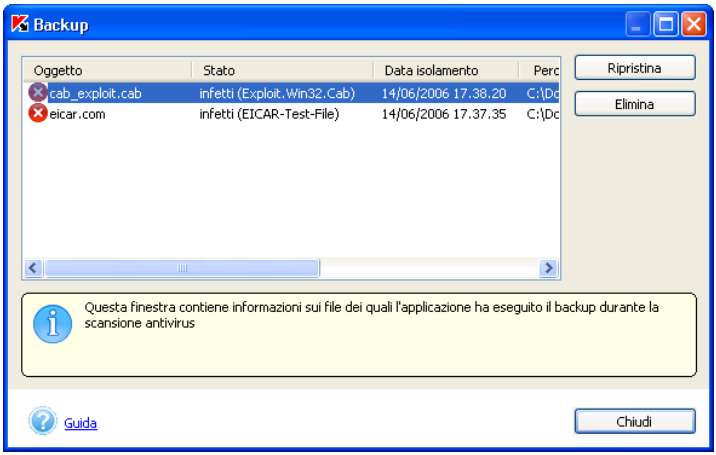

Figura 51. Finestra Backup

Quando è possibile ripristinare le copie di backup?

A volte, durante la disinfezione di un oggetto, non è possibile preservarne l'integrità. Se il file disinfettato conteneva informazioni importanti che dopo la disinfezione non sono più disponibili, parzialmente o completamente, si può provare a ripristinare l'oggetto originale dalla copia di backup. Si raccomanda di eseguire la scansione antivirus dell'oggetto subito dopo averlo ripristinato. Utilizzando il database antivirus aggiornato, l'applicazione potrebbe essere in grado di disinfettarlo senza danneggiarne l'integrità.

Si sconsiglia di ripristinare le copie di backup di oggetti, a meno che non sia assolutamente necessario. Ciò potrebbe causare l'infezione del computer con un virus.

Per impostazione predefinita, non ci sono restrizioni al periodo massimo di memorizzazione delle copie di backup, né alla dimensione massima della memoria di backup. Si consiglia di esaminare e pulire la memoria di backup regolarmente. È possibile impostare il programma in modo che elimini automaticamente le copie di backup più vecchie e che notifichi il sovraccarico della memoria di backup (vedere la sezione 5.10.1.1 a pagina 103).

5.10.2. Uso dei report

Kaspersky Anti-Virus conserva un rapporto completo relativo ai risultati di tutte le attività completate nella finestra **Report** (vedere la Figura 52), che può essere esaminata facendo clic sul collegamento Visualizza report nel riquadro sinistro della scheda **Protezione** (vedere la figura 2). È qui che l'applicazione registra lo stato di ogni attività con la data e l'ora del completamento.

Le informazioni sullo stato dell'elaborazione degli oggetti possono appartenere a una delle seguenti categorie:

- or *Messaggio informativo* contenente informazioni di riferimento (ad esempio: *attività in corso, completata, sospesa*).
- *Messaggio di attenzione* contenente informazioni critiche (ad esempio: Attenzione! Rilevati oggetti infetti dopo la scansione).
- *Un messaggio di avvertenza* contenente commenti su alcuni momenti importanti del funzionamento dell'applicazione (ad esempio: interrotta dall'utente).

Di norma, le notifiche di riuscita ed i messaggi informativi hanno un valore puramente indicativo, di importanza non cruciale; è possibile quindi disabilitare la visualizzazione dei report che contengono solo messaggi di questo tipo. Per fare ciò, deselezionare la casella **Mostra report informazioni**. Si noti che i report relativi all'esecuzione di un'attività specifica contrassegnati con l'icona saranno sempre visualizzati.

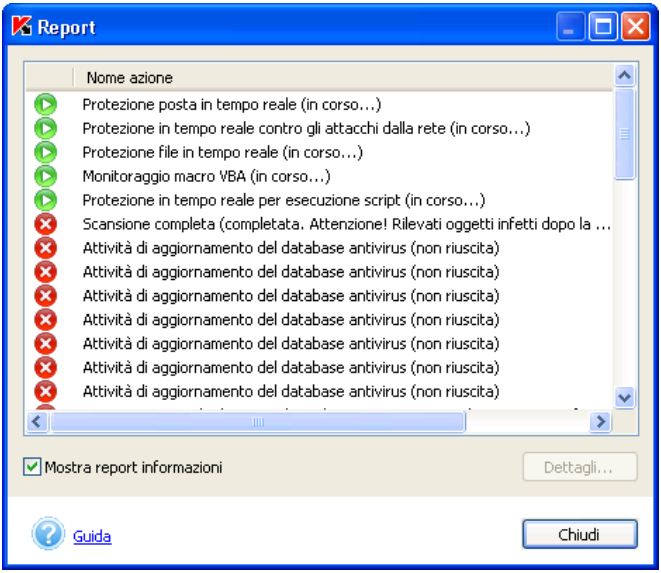
Report
Nome azione
Protezione posta in tempo reale (in corso...)
Protezione in tempo reale contro gli attacchi dalla rete (in corso...)
Protezione file in tempo reale (in corso...)
Monitoraggio macro VBA (in corso...)
Protezione in tempo reale per esecuzione script (in corso...)
Scansione completa (completata. Attenzione! Rilevati oggetti infetti dopo la ...
Attività di aggiornamento del database antivirus (non riuscita)
Attività di aggiornamento del database antivirus (non riuscita)
Attività di aggiornamento del database antivirus (non riuscita)
Attività di aggiornamento del database antivirus (non riuscita)
Attività di aggiornamento del database antivirus (non riuscita)
Attività di aggiornamento del database antivirus (non riuscita)
Attività di aggiornamento del database antivirus (non riuscita)
Mostra report informazioni
Dettagli...
Guida
Chiudi

Figura 52. La finestra **Report**

Questa finestra consente inoltre di ordinare i report disponibili per tipo, nome (in ordine alfabetico) od ora di completamento dell'attività a cui si riferiscono. Per ordinare i report elencati nella finestra secondo uno dei suddetti criteri, fare clic sull'intestazione della colonna corrispondente.

Questa finestra consente di eseguire le seguenti azioni tramite il menu di scelta rapida (che si apre facendo clic col tasto destro del mouse sul nome del report):

- **Esporta report dettagliato su file** Utilizzando la finestra di dialogo standard di Windows che verrà aperta, immettere il nome del file, selezionare la cartella nel quale salvarlo e scegliere il pulsante **Salva**. Il report verrà salvato in formato Microsoft Excel o in formato testo.
- **Invia report a Kaspersky Lab**. È possibile inviare questo report se l'attività (per esempio la scansione del computer o un aggiornamento del database antivirus) è stata interrotta o si è risolta in un errore, e non si conosce il motivo di questo comportamento. Si aprirà automaticamente il client di posta predefinito, ad esempio Microsoft Outlook Express, con un nuovo messaggio al quale sarà allegato il file report. Procedere all'invio del messaggio; gli specialisti di Kaspersky Lab cercheranno di prestare assistenza al più presto.

La creazione automatica dei messaggi di posta elettronica viene sempre eseguita con Microsoft Outlook o Microsoft Outlook Express. Se sul computer è installato un programma diverso per la posta elettronica (ad esempio, The Bat!), sarà necessario configurare il supporto Simple MAPI per il programma per fare sì che questo sia in grado di creare automaticamente messaggi di posta elettronica.

I comandi **Elimina report** e **Elimina tutti i report** consentono rispettivamente di eliminare un report o tutti i report dall'elenco. Non è possibile eliminare un report relativo a un'attività attualmente in corso.

È possibile visualizzare le impostazioni, le statistiche e i report per gli oggetti rilevati per qualsiasi attività selezionata nel registro, tramite le rispettive schede. Per fare ciò, fare clic sul pulsante **Dettagli...**.

Si apre così una finestra contenente un report dettagliato sull'esecuzione dell'attività, comprendente le schede **Statistiche**, **Report** e **Impostazioni**.

La scheda **Statistiche** (vedere la Figura 53) consente all'utente di esaminare le informazioni generali sul lavoro svolto da Kaspersky Anti-Virus per completare l'attività: data e ora di avvio e completamento dell'attività, numero totale di file esaminati e numero di oggetti infetti, disinfettati e messi in quarantena. Quando l'attività di aggiornamento è in corso, la scheda visualizzerà la dimensione totale degli aggiornamenti all'origine, nonché la dimensione degli aggiornamenti scaricati sul computer.

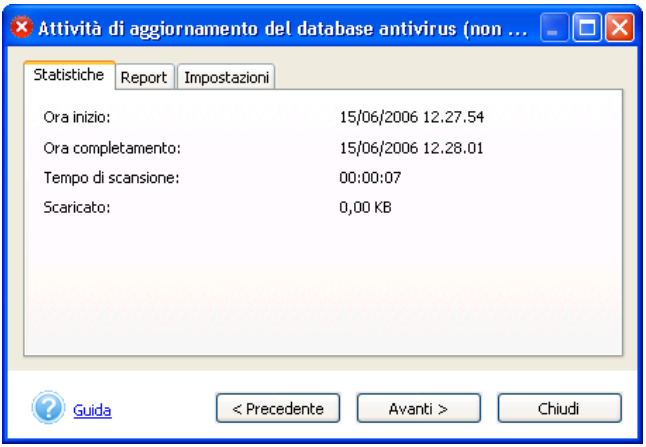

Figura 53. La scheda **Statistiche**

Per impostazione predefinita, la scheda **Report** (vedere la figura 55) non contiene informazioni relative agli oggetti "sani" e visualizza esclusivamente informazioni relative ai virus rilevati. Per visualizzare informazioni sugli oggetti

non infetti, selezionare la casella **Registra tutti i messaggi** nelle impostazioni supplementari di Kaspersky Anti-Virus (vedere la sezione 5.10.4 a pagina 114). In questo caso la scheda visualizzerà informazioni su tutti gli oggetti esaminati. Per le attività di aggiornamento, questa scheda contiene informazioni relative ad ogni passaggio dell'attività: connessione ai server degli aggiornamenti, file scaricati e informazioni sulla loro installazione nel computer. Le informazioni su questa scheda vengono sempre visualizzate, a prescindere dalla selezione o meno della casella **Registra tutti i messaggi** nelle impostazioni supplementari di Kaspersky Anti-Virus.

*Se non si desidera che l'applicazione visualizzi i messaggi informativi per la sessione corrente e non si desidera deselezionare la casella **Registra tutti i messaggi**,*

mentre si stanno visualizzando i report nella scheda **Report** (vedere la figura 55), fare clic con il tasto destro del mouse per aprire il menu di scelta rapida (vedere la Figura 54), e deselezionare la casella **Mostra report dettagliato**.

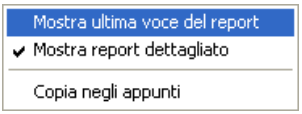

Figura 54. Menu di scelta rapida Report

È inoltre possibile copiare negli appunti informazioni su singoli eventi. Per fare ciò, selezionare l'evento desiderato e scegliere il comando **Copia negli appunti** dal menu di scelta rapida.

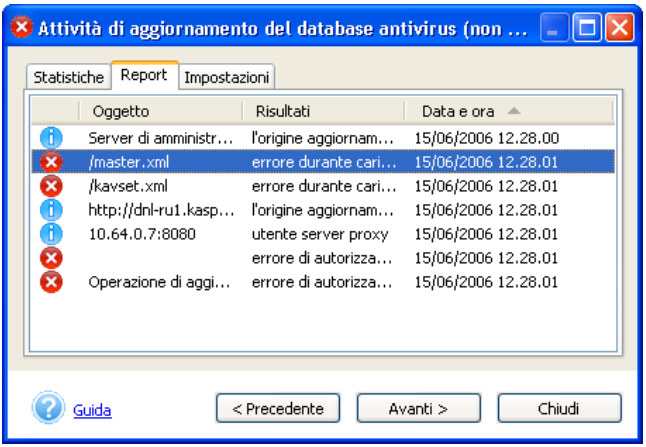

Figura 55. La scheda **Report**

La scheda **Impostazioni** (vedere la figura 56) visualizza le impostazioni dell'attività. Essa contiene informazioni sugli oggetti da esaminare, il livello di protezione selezionato per l'attività e le azioni che l'applicazione eseguirà sugli oggetti infetti, i programmi pericolosi ed i file possibilmente infetti.

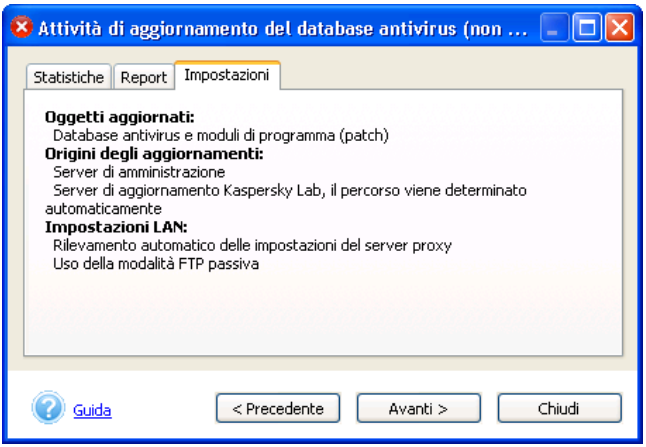

Figura 56. La scheda **Impostazioni**

È possibile selezionare le attività da visualizzare nel Registro attività o direttamente nella finestra dei report dettagliati tramite i pulsanti **Avanti** e **Indietro** oppure facendo clic sul nome dell'attività nel corrispondente elenco a discesa.

È possibile configurare le impostazioni per il registro dei report nella finestra **Impostazioni supplementari** (vedere la Figura 58), che viene visualizzata facendo clic sul corrispondente collegamento nel riquadro sinistro della scheda **Impostazioni** (per dettagli, vedere la sezione 5.10.4 a pagina 114).Questa finestra consente di definire la durata massima di archiviazione dei report e di abilitare/disabilitare l'inclusione di messaggi informativi nel report dettagliato.

5.10.3. Gestione della configurazione di Kaspersky Anti-Virus

Kaspersky Anti-Virus consente di creare ed utilizzare diverse configurazioni per il suo funzionamento. Ora è possibile configurare una determinata modalità di funzionamento dell'applicazione, salvarne le impostazioni in un file di configurazione speciale, detto *profilo*, e utilizzarle secondo necessità.

Per passare alla gestione della configurazione del programma, utilizzare il collegamento Gestione configurazione nella sezione sinistra della scheda **Impostazioni** (vedere la figura 3).

La finestra che si aprirà (vedere la figura 57) consente, scegliendo il pulsante **Salva profilo**, di salvare le impostazioni correnti dell'applicazione in un file di configurazione speciale, oppure, scegliendo il pulsante **Carica profilo**, di applicare le impostazioni di un file di configurazione creato in precedenza al funzionamento di Kaspersky Anti-Virus. Il caricamento delle impostazioni potrebbe richiedere il riavvio del computer, poiché alcune modalità vengono lanciate all'avvio del sistema operativo.

Per ripristinare le impostazioni raccomandate, scegliere il pulsante **Ripristina profilo...**.

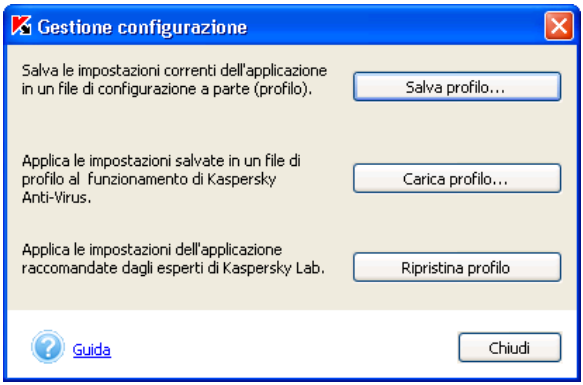
Gestione configurazione
Salva le impostazioni correnti dell'applicazione in un file di configurazione a parte (profilo).
Salva profilo...
Applica le impostazioni salvate in un file di profilo al funzionamento di Kaspersky Anti-Virus.
Carica profilo...
Applica le impostazioni dell'applicazione raccomandate dagli esperti di Kaspersky Lab.
Ripristina profilo
Guida
Chiudi

Figura 57. Gestione configurazione

5.10.4. Impostazioni supplementari

Oltre a configurare le impostazioni di attività specifiche, Kaspersky Anti-Virus consente di configurare varie impostazioni generali e di assistenza (vedere la Figura 58).

Per configurare le impostazioni supplementari di Kaspersky Anti-Virus,

utilizzare il collegamento Impostazioni supplementari nella sezione sinistra della scheda **Impostazioni** (vedere la figura 3). Si aprirà una finestra contenente le schede **Generale**, **Efficienza** e **Sicurezza**.

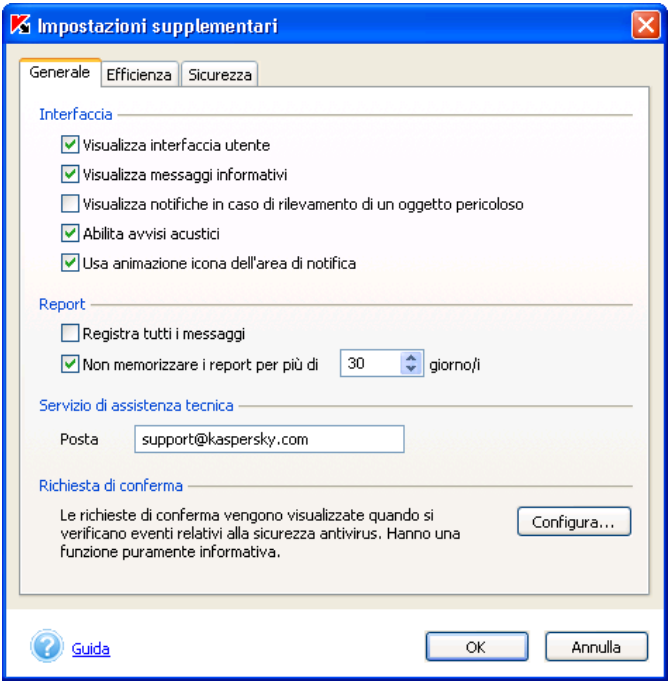

Figura 58. Impostazioni supplementari di Kaspersky Anti-Virus. La scheda **Generale**

La scheda **Generale** (vedere la Figura 58) offre le seguenti opzioni:

- **Visualizza interfaccia utente** - consente la visualizzazione dell'icona dell'applicazione nell'area di notifica e di avviare la finestra principale dell'applicazione in modalità utente (vedere la 5.10.7 a pagina 120).

  Le impostazioni di visualizzazione dell'interfaccia utente verranno applicate solo dopo il riavvio del computer.

- **Visualizza messaggi informativi** - consente la visualizzazione di tutti messaggi che accompagnano il funzionamento di Kaspersky Anti-Virus. I messaggi verranno visualizzati sopra l'icona dell'applicazione nell'area di notifica

  La visualizzazione dei messaggi informativi non è disponibile con i sistemi operativi Microsoft Windows 98 o Microsoft Windows NT Workstation 4.0.

- **Visualizza notifiche in caso di rilevamento di un oggetto pericoloso** - consente di visualizzare messaggi informativi relativi al rilevamento di oggetti pericolosi.
- **Abilita avvisi acustici** - consente la notifica tramite segnali acustici degli eventi che si verificano durante il funzionamento di Kaspersky Anti-Virus. È possibile visualizzare l'elenco di eventi e modificare l'insieme di file audio corrispondente a tali eventi utilizzando gli strumenti standard di Windows (**Start** → →**Pannello di controllo** → **Suoni e periferiche audio**→ **Suoni**).
- **Usa animazione icona dell'area di notifica** - abilita l'animazione dell'icona in funzione dell'operazione eseguita da Kaspersky Anti-Virus. Ad esempio, durante la scansione di un messaggio di posta elettronica, viene visualizzata un'icona di busta lampeggiante.
- **Registra tutti i messaggi** - consente la registrazione di tutti i messaggi generati durante il funzionamento dell'applicazione: messaggi informativi, messaggi di errore, e così via. Questa modalità è disattivata per impostazione predefinita, e vengono registrati solo i messaggi importanti, quali quelli che notificano che l'operazione eseguita dall'applicazione è terminata con un errore, o l'interruzione di un'attività, ecc.
- **Non memorizzare i report per più di... giorno/i** Per impostazione predefinita, i report vengono conservati per 30 giorni. È possibile modificare il periodo di memorizzazione inserendo il valore desiderato nel campo sulla destra della casella, oppure deselezionandola. Verrà eseguita una ricerca dei report memorizzati oltre il periodo di memorizzazione specificato, e quelli obsoleti verranno eliminati all'avvio di Kaspersky Anti-Virus.

È possibile specificare l'indirizzo del Servizio di assistenza tecnica nella sezione **Servizio di assistenza tecnica**. Per impostazione predefinita, viene utilizzato l'indirizzo di posta elettronica del Servizio di assistenza tecnica di Kaspersky Lab: (support@kaspersky.com). Utilizzando questo campo è possibile, ad esempio, specificare l'indirizzo dell'amministratore della sicurezza, oppure un URL che si aprirà quando si richiede assistenza.

La sezione **Richiesta di conferma** consente di definire se visualizzare o meno le notifiche relative agli eventi verificatisi durante il funzionamento di Kaspersky Anti-Virus. Di regola, tutte le notifiche hanno valore puramente indicativo. Per dettagli sulla configurazione delle richieste di conferma, vedere la sezione 5.10.5 a pagina 119).

È possibile configurare restrizioni da imporre alla scansione manuale per ridurre il consumo della batteria (se si sta utilizzando un computer portatile) e delle risorse del sistema operativo (per dettagli vedere la sezione 5.10.6 a pagina 120) sulla scheda **Efficienza** (vedere la Figura 59).

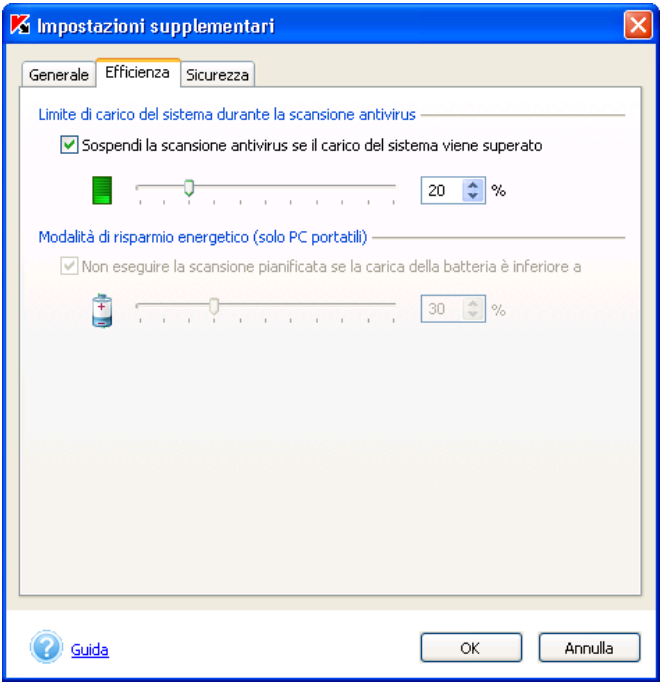

Figura 59. Impostazioni supplementari di Kaspersky Anti-Virus
La scheda **Efficienza**

La scheda **Sicurezza** (vedere la Figura 61) contiene le seguenti impostazioni:

- **Esegui Kaspersky Anti-Virus all'avvio del sistema** - consente l'esecuzione automatica di Kaspersky Anti-Virus all'avvio del sistema.

  Si raccomanda di non disabilitare tale impostazione, poiché ciò potrebbe causare l'infezione del computer con un virus.

  Non sarà possibile accedere a questa impostazione se non si dispone di diritti di amministratore per il computer.

- **Usa recupero dopo errori di sistema** - abilita il sistema di recupero di Kaspersky Anti-Virus in caso di errore durante il suo funzionamento. Se si è verificato un errore durante il funzionamento dell'applicazione, la finestra principale di Kaspersky Anti-Virus si minimizzerà (se era aperta) e verrà visualizzato un messaggio informativo sopra l'icona nell'area di notifica (vedere la Figura 60), dopodiché il funzionamento dell'applicazione sarà recuperato.

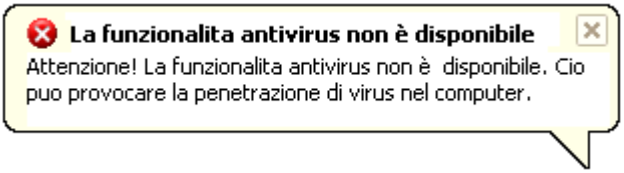
La funzionalita antivirus non è disponibile
Attenzione! La funzionalita antivirus non è disponibile. Cio puo provocare la penetrazione di virus nel computer.

Figura 60. Errore di funzionamento.

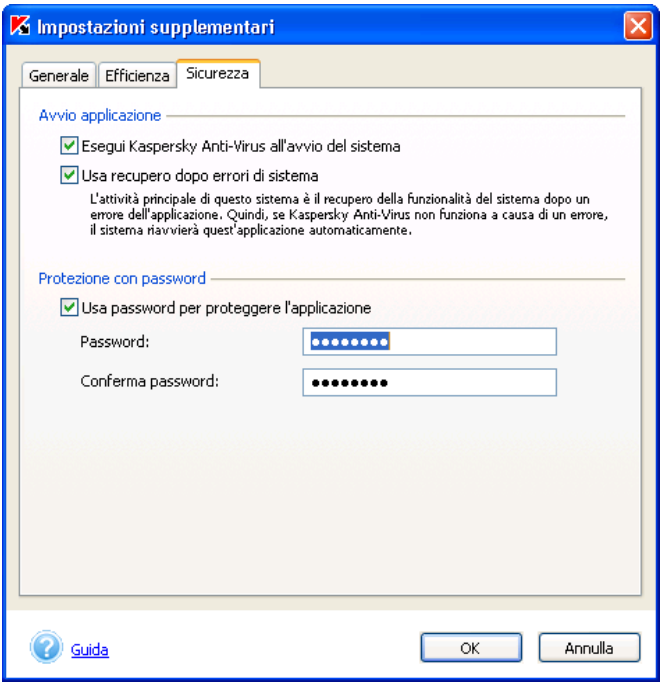
Impostazioni supplementari
Generale
Efficienza
Sicurezza
Avvio applicazione
Esegui Kaspersky Anti-Virus all'avvio del sistema
Usa recupero dopo errori di sistema
L'attività principale di questo sistema è il recupero della funzionalità del sistema dopo un errore dell'applicazione. Quindi, se Kaspersky Anti-Virus non funziona a causa di un errore, il sistema riavvierà quest'applicazione automaticamente.
Protezione con password
Usa password per proteggere l'applicazione
Password:
Conferma password:
Guida
OK
Annulla

Figura 61. Impostazioni supplementari di Kaspersky Anti-Virus
La scheda **Sicurezza**

Usa password per proteggere l'applicazione - abilita la richiesta della password quando si passa alla modalità amministratore. Si consiglia di utilizzare questa modalità se ci sono altri utenti che hanno accesso al computer e si desidera impedire che possano modificare le impostazioni di protezione antivirus, disabilitare la protezione in tempo reale o chiudere Kaspersky Anti-Virus (per dettagli vedere la sezione 5.10.7 a pagina 120). Quando si abilita questa modalità, immettere il numero di caratteri necessario nel campo **Password:** e re-inserirli nel campo **Conferma password**.

5.10.5. Configurazione delle richieste di conferma

Se si desidera essere informati di certi eventi che si verificano durante il funzionamento di Kaspersky Anti-Virus, seguire il collegamento Impostazioni supplementari nella sezione sinistra della scheda **Impostazioni** (vedere la figura 3). Nella finestra di configurazione delle impostazioni supplementari che verrà aperta, scegliere il pulsante **Configura** nella sezione **Richiesta di conferma**. Verrà visualizzata una finestra di dialogo dove sarà possibile configurare le richieste di conferma (vedere la figura 62).

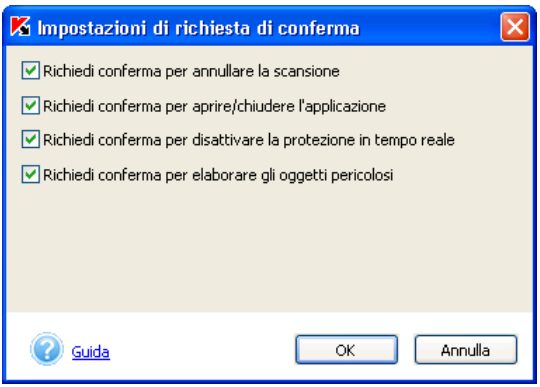
Impostazioni di richiesta di conferma
Richiedi conferma per annullare la scansione
Richiedi conferma per aprire/chiudere l'applicazione
Richiedi conferma per disattivare la protezione in tempo reale
Richiedi conferma per elaborare gli oggetti pericolosi
Guida
OK
Annulla

Figura 62. Configurazione delle richieste di conferma

I seguenti eventi possono essere associati a richieste di conferma:

- **Richiedi conferma per annullare la scansione** - visualizza una richiesta di conferma quando si annulla una scansione manuale. Se la scansione è stata annullata, sopra l'icona dell'applicazione nell'area di notifica verrà visualizzato un messaggio a comparsa contenente le ragioni per cui la scansione è stata annullata.
- **Richiedi conferma per aprire/chiudere l'applicazione** - visualizza una richiesta di conferma all'apertura/chiusura di Kaspersky Anti-Virus.
- **Richiedi conferma per disattivare la protezione in tempo reale** - visualizza un avviso per notificare all'utente che la protezione del computer è stata completamente disabilitata nelle impostazioni della protezione in tempo reale.
- **Richiedi conferma per elaborare gli oggetti pericolosi** - visualizza un avviso per notificare all'utente che sono rimasti oggetti infetti non trattati dopo la scansione antivirus.

5.10.6. Limitare l'efficienza di Kaspersky Anti-Virus

È possibile imporre restrizioni al lancio della scansione manuale se si ritiene necessario limitare l'utilizzo delle risorse del computer. Per fare ciò, seguire il collegamento Impostazioni supplementari nella sezione sinistra della scheda **Impostazioni** (vedere la figura 3). Nella finestra delle impostazioni supplementari dell'applicazione che verrà aperta, passare alla scheda **Efficienza** (vedere la Figura 59).

È possibile imporre le seguenti restrizioni:

- **Sospendi la scansione antivirus se il carico del sistema viene superato** - sospende la scansione antivirus manuale se il carico del file system supera il livello specificato. Quando il carico sul file system scende al livello consentito, la scansione riprende. Specificare il livello di carico consentito sul file system (in percentuale) sopra al quale le scansioni pianificate non possono essere avviate, utilizzando il cursore o il campo di immissione alla sua destra.

  Questa impostazione si applica solo alle scansioni manuali (ad esempio, alla scansione di oggetti selezionati). Ciò non avrà effetto sulla protezione antivirus in tempo reale.

- **Non eseguire la scansione pianificata se la carica della batteria è inferiore a** - annulla le scansioni pianificate se si sta utilizzando un computer portatile e la carica della batteria è inferiore al valore specificato. Specificare il livello di carica della batteria consentito (in percentuale) sotto al quale le scansioni pianificate non possono essere avviate, utilizzando il cursore o il campo di immissione alla sua destra.

  Questa impostazione è disponibile solo se Kaspersky Anti-Virus è installato su un computer portatile alimentato dalla batteria.

5.10.7. Funzionamento in modalità amministratore e modalità utente

Kaspersky Anti-Virus può funzionare in due modalità: modalità amministratore e modalità utente. L'utilizzo di queste modalità può essere preferibile se ci sono altri utenti che hanno accesso al computer. Sarà possibile impedire agli altri utenti di modificare le impostazioni antivirus, disabilitare la protezione in tempo reale o chiudere Kaspersky Anti-Virus. In modalità utente, l'interfaccia dell'applicazione è diversa e le impostazioni non disponibili saranno nascoste

(per esempio, la scheda **Impostazioni** non sarà visualizzata nella finestra principale dell'applicazione).

È possibile abilitare l'utilizzo delle modalità utente e amministratore utilizzando l'interfaccia locale o l'applicazione Kaspersky Administration Kit (vedere la sezione 6.1.2.14 a pagina 150).

Per abilitare l'utilizzo delle modalità utente e amministratore tramite l'interfaccia locale,

Selezionare la casella **Usa password per proteggere l'applicazione** nella scheda **Sicurezza** (vedere la Figura 61) della finestra delle impostazioni supplementari di Kaspersky Anti-Virus. Immettere la password nel campo **Password** e reinserirla nel campo **Conferma password**.

Il menu di scelta rapida dell'applicazione visualizzerà allora il comando **Passa alla modalità utente** (vedere la figura 1). Questo comando consente di passare alla modalità utente. Per tornare alla modalità amministratore, utilizzare il comando **Passa alla modalità amministratore** del menu di scelta rapida ed inserire la password nella finestra di dialogo che verrà visualizzata (vedere la figura 63).

Se la casella **Usa password per proteggere l'applicazione** (vedere la Figura 61) non è selezionata, Kaspersky Anti-Virus si aprirà e funzionerà in modalità amministratore.

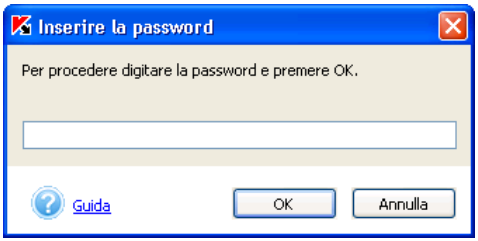

Figura 63. Inserimento della password

Per nascondere completamente l'interfaccia dell'applicazione mentre l'applicazione è in modalità utente,

selezionare la casella **Visualizza interfaccia utente** nella scheda **Generale** (vedere la Figura 58) della finestra delle impostazioni supplementari di Kaspersky Anti-Virus.

In questo caso l'icona di Kaspersky Anti-Virus non sarà visualizzata nell'area di notifica, né si aprirà la finestra principale dell'applicazione.

CAPITOLO 6. GESTIONE DELL'APPLICAZIONE TRAMITE KASPERSKY ADMINISTRATION KIT

6.1. Gestione delle regole

Questa sezione descrive le modalità di creazione e gestione delle regole per Kaspersky Anti-virus. Per istruzioni dettagliate sulla gestione delle regole, consultare il manuale dell'amministratore di Kaspersky Administration Kit 5.0.

6.1.1. Creazione di una regola

Per creare una nuova regola, eseguire le seguenti azioni:

1. Nel nodo **Gruppi** della struttura della consolle, selezionare il gruppo di computer al quale si vuole assegnare la nuova regola.
2. In tale gruppo, selezionare la cartella **Regole**, aprire il menu di scelta rapida e fare clic su **Nuovo →Regola…** per dare inizio alla procedura di creazione guidata di una nuova regola.

L'applicazione di creazione delle nuove regole è organizzata come una procedura guidata di Windows, che guida l'utente attraverso il processo. Per navigare tra le finestre di dialogo della procedura, usare i pulsanti **< Indietro** e **Avanti >**. Per terminare la procedura, fare clic su **Fine**. Per annullare la procedura in qualsiasi momento, fare clic su **Annulla**.

Durante le fasi di creazione di una regola, verrà configurato un insieme minimo di impostazioni, senza il quale l'applicazione non può funzionare. Altri valori verranno impostati per impostazione predefinita, e corrisponderanno ai valori predefiniti dell'installazione locale dell'applicazione. La regola può essere modificata (vedere la 6.1.2 a pagina 126).

Durante la creazione di regole (Fase 2. – Fase 5.) è possibile proibire la modifica delle impostazioni delle regole dei gruppi nidificati e delle impostazioni di applicazioni ed attività. Per disabilitare la modifica delle impostazioni, è possibile "bloccarle": . Le impostazioni di cui è consentita la modifica saranno allora identificate dall'icona .

Fase 1. Immissione delle informazioni generali sulla regola

Le prime finestre di dialogo della procedura guidata sono fasi introduttive, che prevedono l'inserimento del nome della regola nel campo **Nome** e la selezione del prodotto **Kaspersky Anti-Virus 5.0 for Windows Workstations** dall'elenco a discesa **Scegliere l'applicazione per cui definire una regola**. Se si desidera che la regola che si sta creando sia la regola attiva per l'applicazione, attivare la regola selezionando la casella **Attiva regola** nella corrispondente finestra di dialogo della procedura guidata.

È possibile definire diverse regole con diverse impostazioni per un'applicazione, includendole in un gruppo. Tuttavia, solo una regola può essere quella corrente per l'applicazione. È possibile attivare una regola che non è attualmente quella attiva, tramite un evento che consente di applicare impostazioni di protezione antivirus più rigide nei periodi di epidemie informatiche.

Fase 2. Definire il livello di protezione antivirus per la protezione in tempo reale

Questa fase prevede la definizione del livello di protezione antivirus per le attività di protezione in tempo reale (vedere la 4.2 a pagina 36).

Fase 3. Definire il livello di protezione antivirus per la scansione manuale

Questa finestra di dialogo consente di definire il livello di protezione antivirus per la nuova regola (vedere la sezione 4.2 a pagina 36), che sarà utilizzata durante l'esecuzione delle attività di scansione manuale, e di specificare le azioni che saranno eseguite in caso di rilevamento di un oggetto infetto o sospetto (vedere la sezione 5.3.3.2 a pagina 82).

Scegliendo il pulsante **Dettagli** si apre una finestra contenente le impostazioni avanzate della modalità di scansione manuale (vedere la Figura 68). Modificando una qualsiasi delle impostazioni predefinite, il livello di protezione passerà allo stato **Personalizzato**.

Fase 4. Selezionare l'origine degli aggiornamenti

Durante questa fase (vedere la Figura 64), verrà richiesto di impostare i parametri per l'aggiornamento del database antivirus e dei moduli dell'applicazione. La finestra che si apre facendo clic sul pulsante **Impostazioni LAN** consente di specificare l'origine degli aggiornamenti e definire le impostazioni di rete. Tutti le impostazioni sono identiche alle impostazioni locali. Informazioni dettagliate su questo argomento sono reperibili nella sezione 5.1.3 a pagina 42.

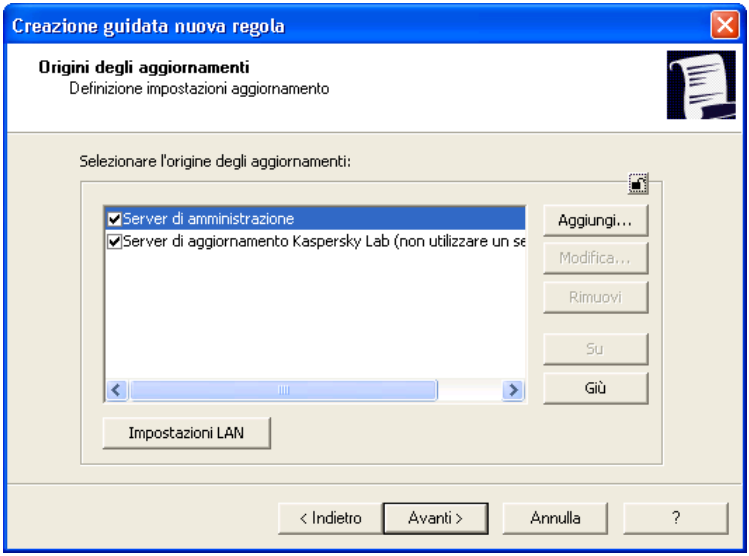

Figura 64. Selezione dell'origine di aggiornamento

Fase 5. Definire i parametri d'aggiornamento

Questa finestra di dialogo (vedere la Figura 65) consente di selezionare le impostazioni del servizio di aggiornamento per i moduli dell'applicazione. Le impostazioni della procedura di aggiornamento sono identiche a quelle della configurazione locale. Informazioni dettagliate su questo argomento sono reperibili nella sezione 5.1.3 a pagina 42.

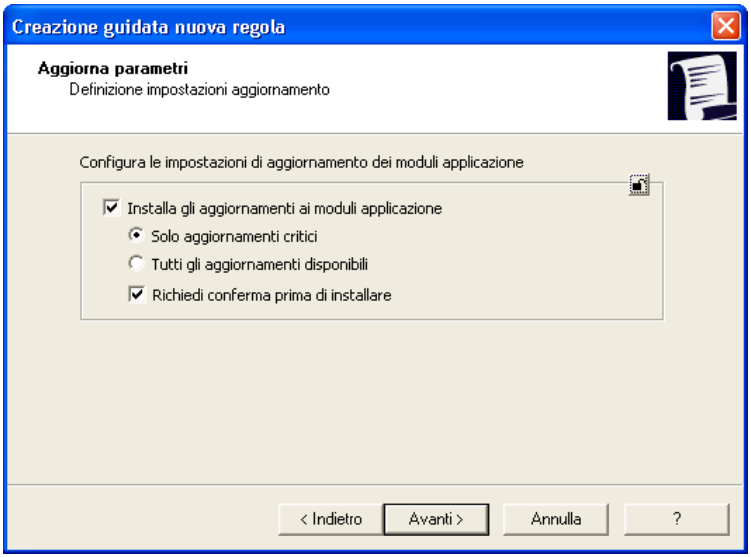

Figura 65. Selezione dei parametri del servizio di aggiornamento

Fase 6. Completare la creazione della regola

La finestra finale della procedura guidata comunica all'utente che una nuova regola è stata creata con successo.

Al termine della procedura, la regola per questa applicazione verrà aggiunta alla cartella **Regole** del gruppo corrispondente, e sarà visualizzata nel pannello dei risultati.

Per applicare la regola, modificarne le impostazioni e specificare le restrizioni alla modifica delle impostazioni delle attività e dell'applicazione qualora non lo si sia ancora fatto durante la creazione della regola. La regola verrà applicata ai computer client al momento della loro prima sincronizzazione con il server di amministrazione.

Una regola viene applicata come segue: in caso di attività residenti (ad esempio, protezione in tempo reale) in esecuzione su un computer client, queste continueranno ad operare con le nuove impostazioni della regola. Le attività periodiche in corso, come la scansione manuale o l'aggiornamento, continueranno a usare le vecchie impostazioni. In questo caso, le modifiche saranno applicate all'avvio successivo dell'applicazione.

È possibile, gestire, copiare e spostare le regole da un gruppo a un altro tramite i normali comandi nel menu di scelta rapida, come **Copia/Incolla**, **Taglia/Incolla**,

e **Cancella**, o tramite comandi analoghi nel menu **Azione**. Per spostare una regola, è sufficiente trascinarne l'icona nella nuova posizione con il mouse.

6.1.2. Visualizzazione e modifica delle impostazioni delle regole

In fase di modifica, è possibile personalizzare le impostazioni delle regole, proibire modifiche a carico delle stesse per i gruppi nidificati, e bloccare le impostazioni di applicazioni e attività in modo che gli utenti non possano modificarle.

Per bloccare le impostazioni di configurazione e impedirne la modifica, contrassegnare le stesse con l'icona di "blocco": . Le impostazioni che possono essere modificate sono contrassegnate da .

Per visualizzare e/o modificare le impostazioni correnti delle regole:

1. Nella cartella **Gruppi** della struttura della consolle, selezionare il gruppo di computer per il quale si desidera modificare le impostazioni delle regole.
2. Selezionare la cartella **Regole** di questo gruppo. Tutte le regole disponibili per il gruppo saranno visualizzate nel pannello dei risultati.
3. Nell'elenco di regole, scegliere una regola per **Kaspersky Anti-Virus 5.0 for Windows Workstations** (il nome dell'applicazione è visualizzato nel campo **Applicazione**).
4. Aprire il menu di scelta rapida della regola selezionata e fare clic su **Proprietà**. Si apre una finestra con le proprietà della regola per **Kaspersky Anti-Virus 5.0 for Windows Workstations**, contenente diverse schede.

Le schede **Generale**, **Imposizione** e **Elaborazione evento** sono schede standard di Kaspersky Administration Kit (per dettagli, vedere la guida di Kaspersky Administration Kit 5.0).

Le schede rimanenti visualizzano impostazioni specifiche di Kaspersky Anti-Virus 5.0 for Windows Workstations. Queste schede sono descritte più dettagliatamente di seguito.

6.1.2.1. Visualizzazione delle informazioni sulla regola

La scheda **Generale** (vedere la figura 66) visualizza informazioni generali sulla regola:

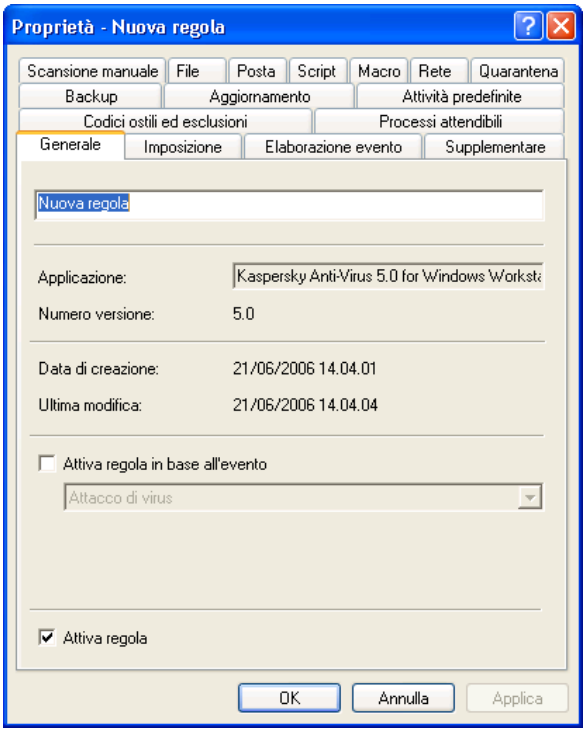

Figura 66. La scheda **Generale**

- Nome della regola;
- Applicazione a cui la regola è stata assegnata (**Kaspersky Anti-Virus 5.0 for Windows Workstations**);
- Versione dell'applicazione;
- Data e ora di creazione;
- Data e ora dell'ultima modifica.

Questa scheda consente di modificare il nome della regola.

Per attivare la regola, selezionare la casella **Attiva regola**. Se si desidera attivare la regola automaticamente in concomitanza con un determinato evento, selezionare la casella **Attiva regola in base all'evento** e selezionare l'evento desiderato dall'elenco a discesa. È possibile tornare alla precedente regola solo manualmente.

6.1.2.2. Scansione manuale

Per configurare le impostazioni della regola per le scansioni manuali, utilizzare la scheda **Scansione manuale** (vedere la Figura 67).

Nella sezione **Configurazione del livello di protezione** (vedere la sezione 4.2 a pagina 36), selezionare uno dei tre livelli di protezione antivirus predefiniti dall'elenco la discesa.

La sezione **Azioni da eseguire sugli oggetti rilevati** consente di specificare il tipo di azione da eseguire in caso di rilevamento di un oggetto infetto o sospetto (per dettagli sul tipo di azioni eseguite da Kaspersky Anti-Virus in modalità di scansione manuale, vedere la sezione 5.3.3.2 a pagina 82).

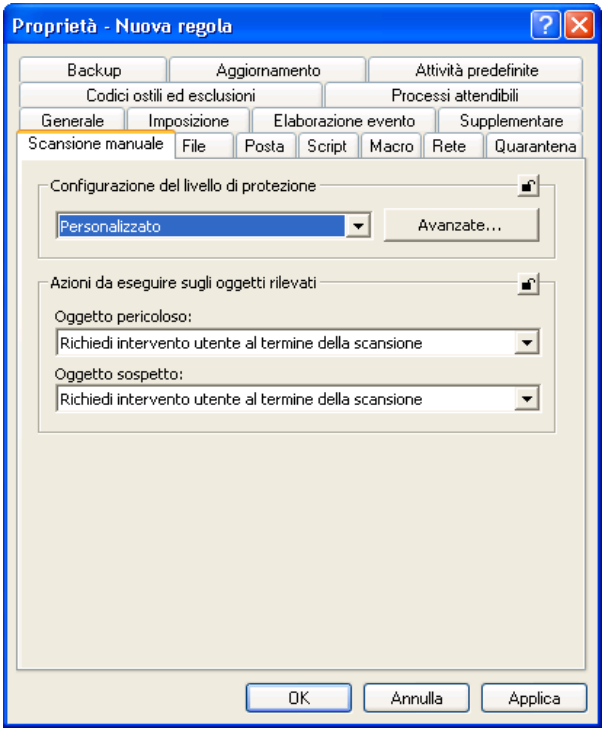

Figura 67. La scheda **Scansione manuale**

Dall'elenco a discesa **Configurazione del livello di protezione**, selezionare uno dei tre livelli di protezione antivirus predefiniti (vedere la sezione 4.2 a pagina 36):

Facendo clic sul pulsante **Avanzate** si apre una finestra che consente di rivedere le impostazioni del livello di protezione antivirus selezionato ed eventualmente personalizzarlo. In quest'ultimo caso, il livello di protezione passa allo stato **Personalizzato**.

La finestra di impostazione avanzata contiene le schede **Definizione scansione** e **Supplementare**.

La scheda **Definizione scansione** (vedere la Figura 68) consente di specificare gli oggetti da esaminare e di definirne il tipo, nonché di definire un elenco di quelli da escludere dalla scansione (per dettagli, vedere la sezione 5.3 a pagina 71).

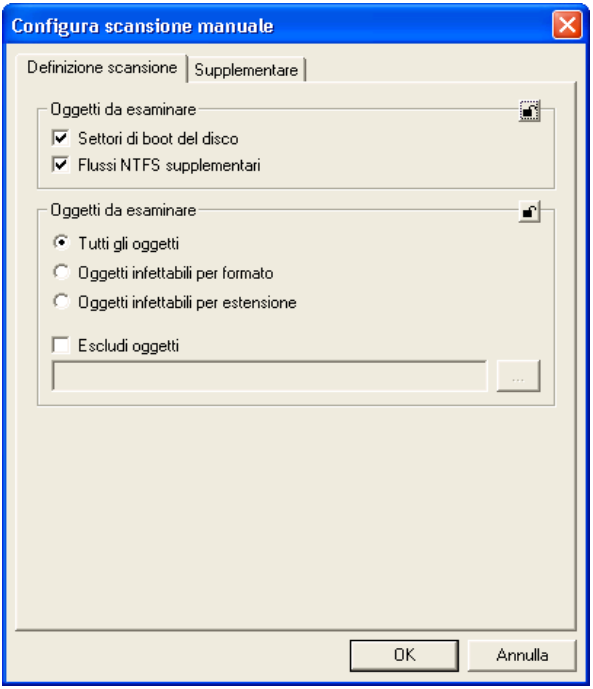

Figura 68. La scheda **Definizione scansione**

La scheda **Supplementare** (vedere la Figura 69) consente di abilitare/disabilitare la scansione di diversi tipi di file compositi, escludere dalla scansione i programmi potenzialmente pericolosi ammessi e abilitare la richiesta di una password per gli archivi criptati o specificare determinate restrizioni per il processo di scansione (per dettagli, vedere la sezione 5.3 a pagina 71).

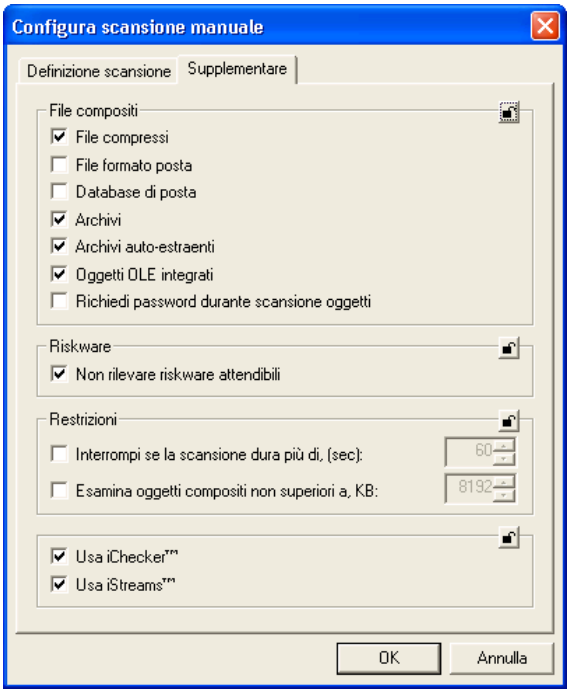

Figura 69. La scheda **Supplementare**

6.1.2.3. Protezione in tempo reale degli oggetti del file system

La scheda **File** (vedere la figura 70) consente di personalizzare le impostazioni delle regole per una protezione costante degli oggetti del file system. Le procedure di selezione del livello di protezione e di accesso alla finestra delle impostazioni avanzate sono identiche a quelle descritte per la scheda **Scansione manuale** (vedere la sezione 6.1.2.2 a pagina 128).

La sezione **Azioni da eseguire sugli oggetti rilevati** consente di specificare il tipo di azione da eseguire in caso di rilevamento di un oggetto infetto o sospetto (per dettagli sul tipo di azioni eseguite da Kaspersky Anti-Virus in modalità di scansione manuale, vedere la sezione 5.2.1.2 a pagina 58).

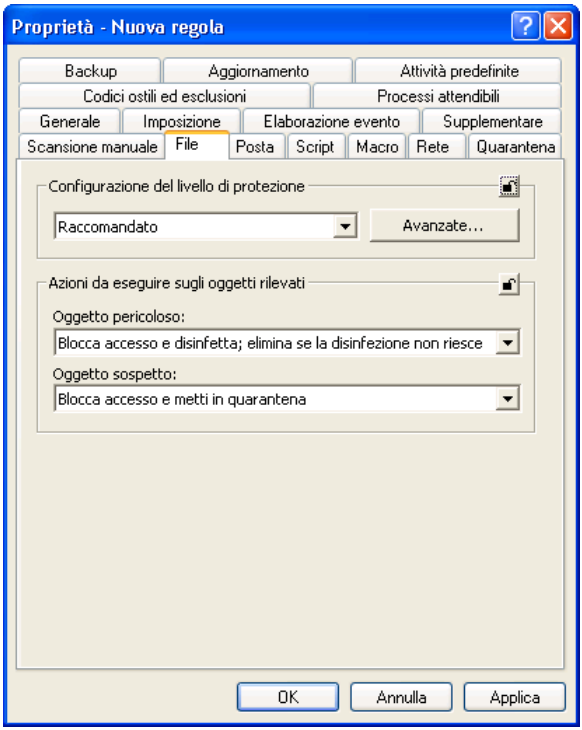

Figura 70. La scheda **File**

Utilizzare la scheda **Definizione scansione** (vedere la Figura 71) per definire gli oggetti da esaminare e quelli esclusi dalla protezione in tempo reale. Questi parametri sono identici a quelli di impostazione locale descritti nella sezione 5.2.1 a pagina 55.

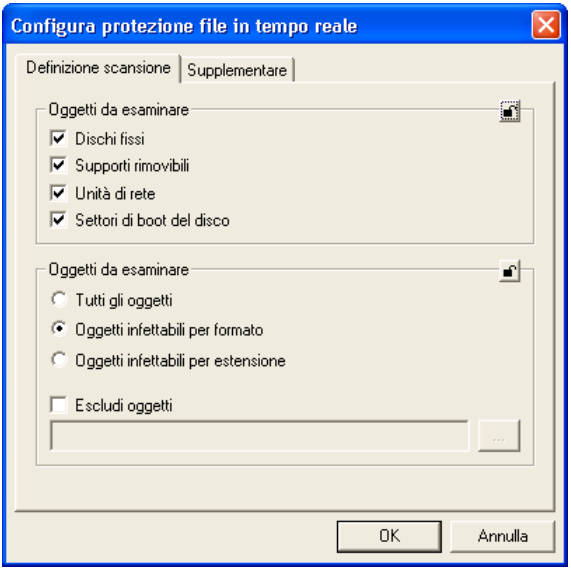

Figura 71. La scheda **Definizione scansione**

La scheda **Supplementare** (vedere la Figura 72) consente di abilitare/disabilitare la scansione di vari tipi di file compositi, escludere dalla scansione i programmi potenzialmente pericolosi ammessi, stabilire limiti di tempo per la scansione ed abilitare/disabilitare le tecnologie iChecker e iStreams (per dettagli, vedere la sezione 5.2.1 a pagina 55).

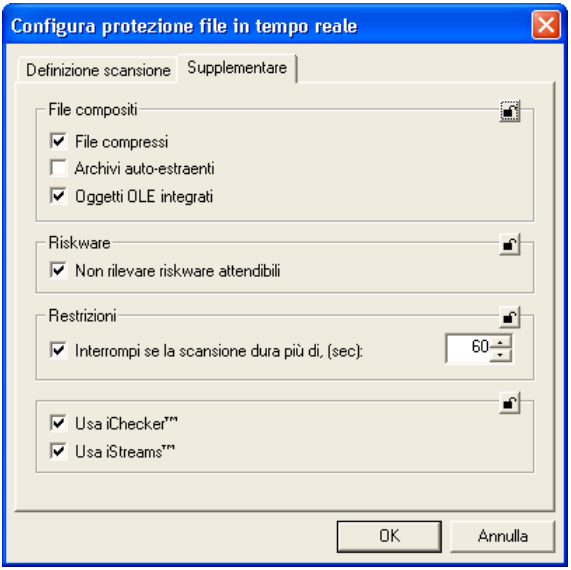

Figura 72. La scheda **Supplementare**

6.1.2.4. Codici ostili ed esclusioni

La scheda **Codici ostili ed esclusioni** (vedere la Figura 73) consente di specificare il tipo di database antivirus (standard o esteso) da utilizzare per le scansioni, nonché di creare un elenco di esclusioni dall'ambito della scansione. Queste impostazioni sono analoghe a quelle dell'interfaccia locale (per dettagli, vedere la sezione 5.1.3.5 a pagina 50 e la sezione 5.7 a pagina 94).

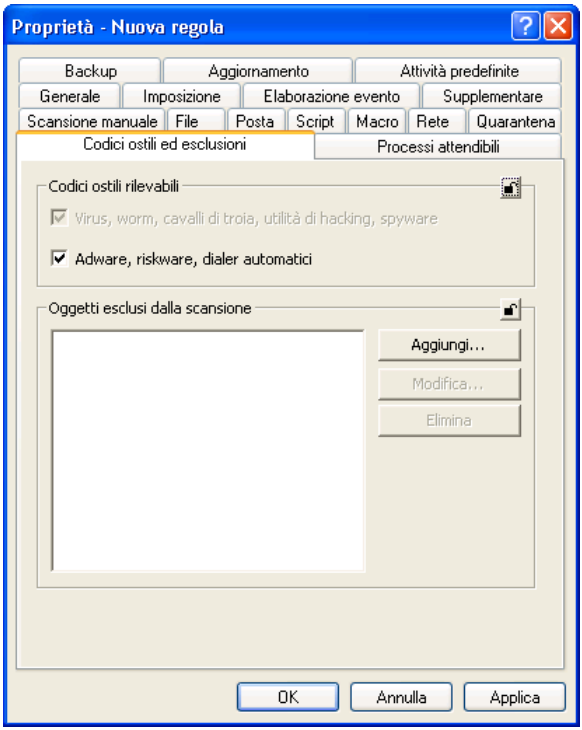

Figura 73. La scheda **Codici ostili ed esclusioni**

6.1.2.5. Monitoraggio dei processi software

Utilizzare la scheda **Processi attendibili** (vedere la Figura 74) per configurare la impostazioni della regola per il monitoraggio antivirus di certi programmi. Queste impostazioni sono analoghe a quelle dell'interfaccia locale (per dettagli, vedere la sezione 5.5 a pagina 91).

Durante l'inserimento del percorso al file, è necessario specificare il percorso del file di processo su un computer remoto.

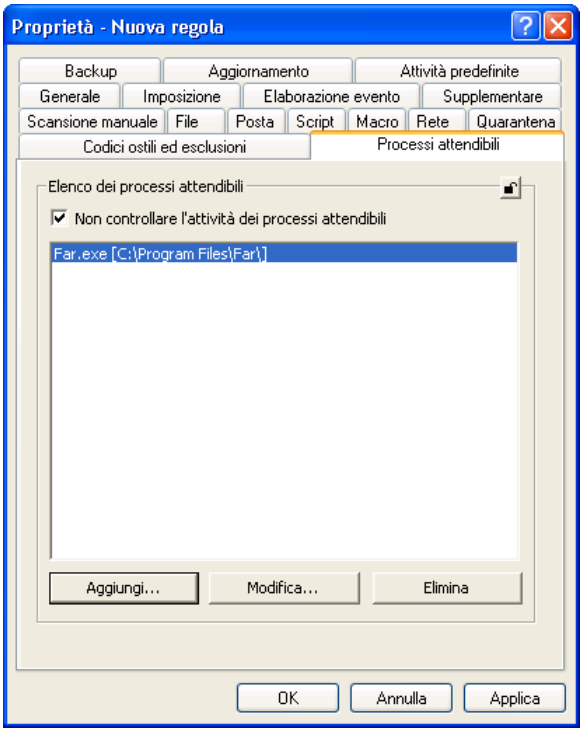

Figura 74. La scheda **Processi attendibili**

6.1.2.6. Scansione dei messaggi di posta elettronica

La scheda **Posta** (vedere la Figura 75) consente di specificare le impostazioni della regola per la scansione dei messaggi di posta elettronica in entrata ed in uscita. Le procedure di selezione del livello di protezione e di accesso alle opzioni di rifinitura sono identiche a quelle descritte per la scheda **Scansione manuale** (vedere la sezione 6.1.2.2 a pagina 128).

La sezione **Azioni da eseguire sugli oggetti rilevati** consente di specificare il tipo di azione da eseguire in caso di rilevamento di un oggetto infetto o sospetto (per dettagli sul tipo di azioni eseguite da Kaspersky Anti-Virus in modalità di scansione manuale, vedere la sezione 5.2.2.2 a pagina 63).

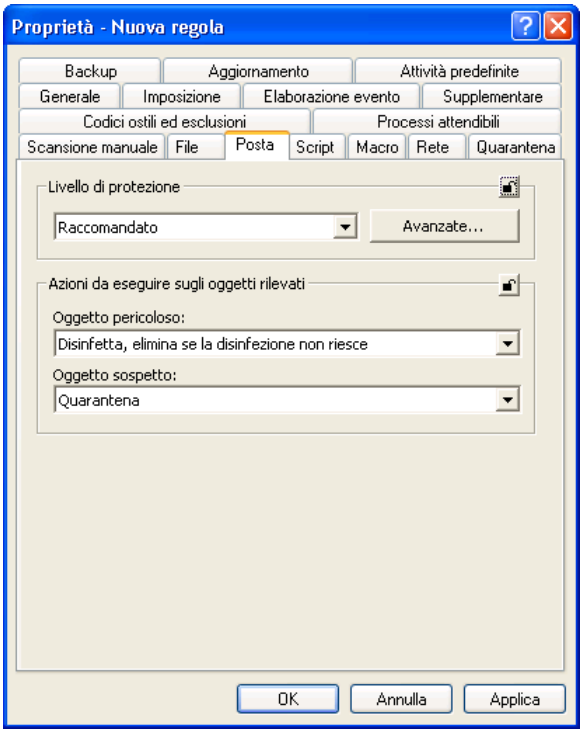

Figura 75. La scheda **Posta**

La sezione **Definizione scansione** (vedere la Figura 76) consente di selezionare gli oggetti da esaminare e specificare il tipo di messaggi di posta elettronica da escludere dalla scansione. Questi parametri sono identici a quelli di impostazione locale. Informazioni dettagliate su questo argomento sono reperibili nella sezione 5.2.2 a pagina 59.

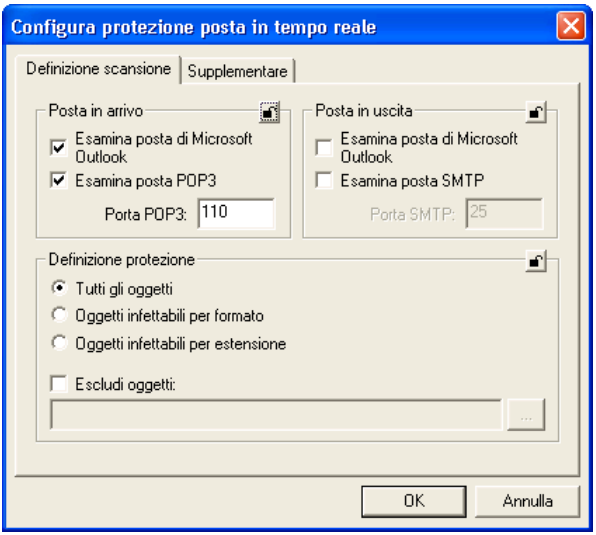

Figura 76. La scheda **Definizione scansione**

La scheda **Supplementare** (vedere la Figura 77) consente di abilitare/disabilitare l'uso della tecnologia iChecker(tm) e di specificare alcune restrizioni per la scansione dei messaggi di posta elettronica (per dettagli, vedere la sezione 5.2.2 a pagina 59).

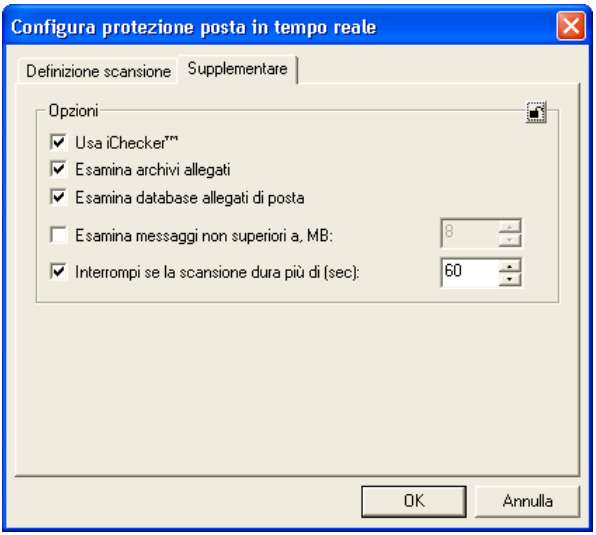

Figura 77. La scheda **Supplementare**

6.1.2.7. Monitoraggio degli script

La scheda **Script** (vedere la Figura 78) consente di impostare i parametri di monitoraggio in tempo reale degli script VBScript e JavaScript potenzialmente pericolosi. Selezionare una delle seguenti opzioni:

- **Blocca esecuzione** (impostazione predefinita);
- **Consenti esecuzione**;
- **Richiedi intervento utente**.

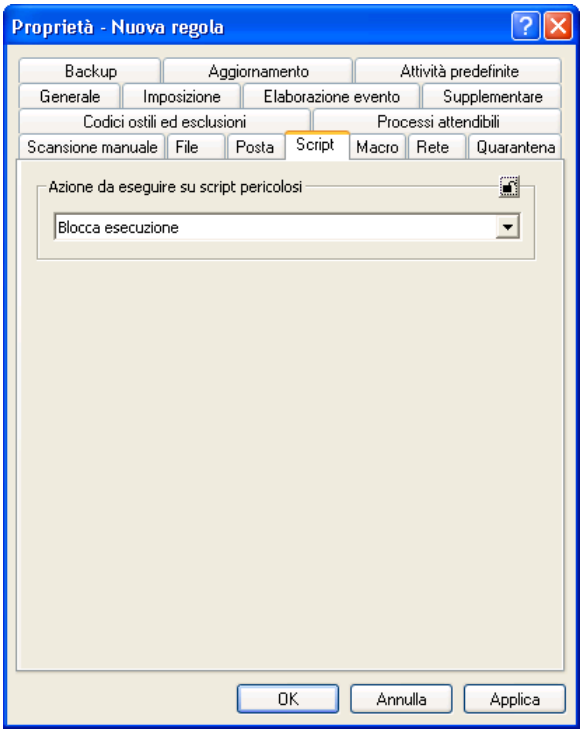

Figura 78. La scheda **Script**

6.1.2.8. Monitoraggio delle macro

La scheda **Macro** (vedere la Figura 79) consente di modificare le impostazioni della regola per il monitoraggio dei comandi macro VBA utilizzati dalle applicazioni di Office.

Le procedure di selezione del livello di protezione e di accesso alla finestra delle impostazioni avanzate sono identiche a quelle descritte per la scheda **Scansione manuale** (vedere la sezione 6.1.2.2 a pagina 128).

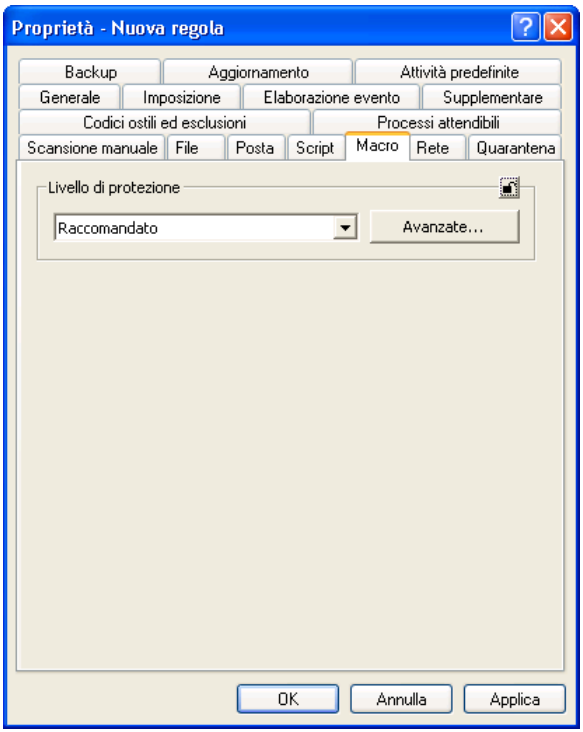

Figura 79. La scheda **Macro**

Fare clic sul pulsante **Avanzate** per aprire una finestra di dialogo (vedere la Figura 80) che elenca i principali tipi di macro monitorate da Kaspersky Anti-Virus.

Cinque tipi di macro sono riportati nelle schede corrispondenti:

- **Moduli** - Macro per il lavoro con moduli di progetto, comprendenti:
  - Moduli di copiatura (OrganizerCopy);

  - Moduli di cancellazione (OrganizerDelete);
  - Moduli di rinomina (OrganizerRename);
  - Modulo di aggiunta;
  - Modulo di eliminazione;
  - Moduli di importazione;
  - Moduli di esportazione.
- **Stringhe** - Macro per la modifica del codice di una macro, comprendenti:
  - Procedura di creazione;
  - Aggiunta di stringhe macro da un file al modulo;
  - Aggiunta di stringhe a una macro;
  - Inserimento di stringhe in una macro;
  - Sostituzione di stringhe in una macro;
  - Eliminazione di stringhe da una macro.
- **File** - Operazioni sui file, comprendenti:
  - Cancellazione di file;
  - Modifica di attributi di file;
  - Creazione di cartelle;
  - Cancellazione di cartelle;
  - Apertura di file in scrittura.
- **ActiveX** - Operazioni con oggetti ActiveX, comprendenti:
  - Creazione di oggetti ActiveX;
  - Creazione di un oggetto ActiveX su un computer remoto;
  - Accesso ad un oggetto ActiveX.
- **Altro** - Altre macro, comprendenti:
  - Disabilitazione della richiesta di salvare il modello Normal;
  - Copia di fogli Excel;
  - Disabilitazione della protezione antivirus;
  - Esecuzione del comando MacroCopy;

- Esecuzione di comandi Shell;
- Chiamata di funzioni API;
- Emulazione di pressione tasti.

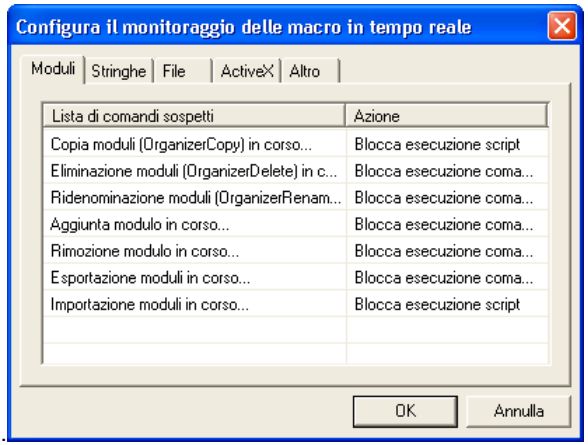

Figura 80. Elenco delle macro

La colonna **Azione** (vedere la Figura 80) visualizza l'azione da applicare (in base al livello di protezione selezionato) alla macro da parte dell'applicazione antivirus. Sono possibili le seguenti azioni:

- *Consenti esecuzione comando macro*.
- *Richiedi intervento utente*.
- *Blocca esecuzione comando macro*.
- *Blocca script* - l'esecuzione dell'intera macro viene interrotta.

Per modificare l'azione che si intende fare eseguire da Kaspersky Anti-Virus sulle macro sospette rilevate:

Fare clic sull'azione e selezionarne una nuova dall'elenco a discesa.

6.1.2.9. Protezione contro gli attacchi di rete

La scheda **Rete** consente di configurare le impostazioni di protezione contro gli attacchi di rete (vedere la Figura 81). Queste impostazioni sono analoghe a quelle dell'interfaccia locale (per dettagli, vedere la sezione 5.2.6 a pagina 69).

Specificare l'azione da eseguire all'aggiornamento del database di protezione contro gli attacchi di rete e quando la protezione contro gli attacchi di rete viene abilitata/disabilitata (vedere la sezione 5.2.6 a pagina 69) nella sezione **Azione in caso sia necessario riavviare il computer**. Selezionare una delle seguenti opzioni:

- *Richiedi intervento utente*. In questo caso, verrà visualizzata una finestra che richiede il riavvio della workstation.
- *Non richiedere intervento utente, rimanda al prossimo avvio* Quest'azione è selezionata per impostazione predefinita.
- *Riavvia ora.* In questo caso, la workstation verrà riavviata subito dopo l'aggiornamento al database degli attacchi di rete.

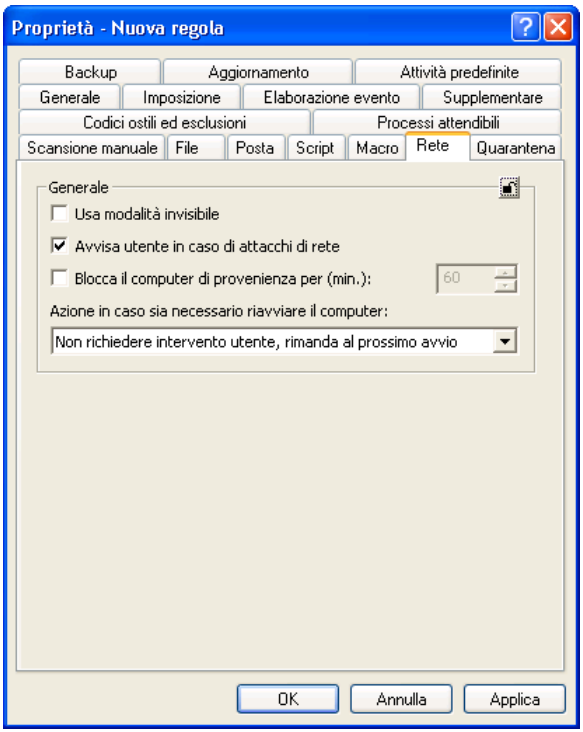

Figura 81. La scheda **Rete**

6.1.2.10. Aggiornamento del database antivirus e dei moduli dell'applicazione

La scheda **Aggiornamento** (vedere la Figura 82) consente di personalizzare le impostazioni di aggiornamento del database antivirus e dei moduli dell'applicazione specificate durante la creazione di una nuova regola.

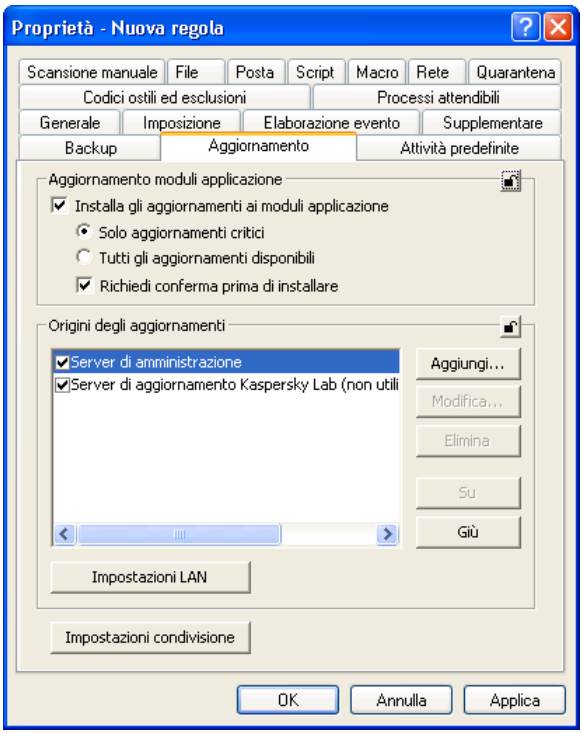

Figura 82. La scheda **Aggiornamento**

La scheda **Aggiornamento** è composta dalle seguenti aree: **Aggiornamento moduli applicazione** - consente di selezionare i parametri del servizio che aggiorna i database antivirus e l'applicazione (vedere la Fase 5. a pagina 124). **Origine degli aggiornamenti** - consente di selezionare l'origine degli aggiornamenti per il database antivirus e i moduli dell'applicazione e di configurarne le impostazioni (vedere lo step 3 a pagina 124).

Il pulsante **Impostazioni LAN** consente di configurare le impostazioni del server proxy (per dettagli, vedere la 5.1.3.4 sezione a pagina 49). Il campo **Time-out connessione (sec.)** nella finestra che verrà aperta consente di stabilire il time-

out per stabilire la connessione con il server degli aggiornamenti (in secondi). Alla scadenza dell'intervallo specificato, l'attività passerà alla successiva origine degli aggiornamenti nell'elenco, o verrà terminata se non sono specificate altre origini degli aggiornamenti.

La finestra che si apre facendo clic sul pulsante **Copiatura impostazioni** consente di copiare gli aggiornamenti su un supporto locale e di configurare le impostazioni di copia (vedere la sezione 5.1.3 a pagina 42).

6.1.2.11. Gestione delle attività di sistema

La scheda **Attività predefinite** (vedere la Figura 83) consente di abilitare/disabilitare il lancio delle attività di sistema pianificate (vedere la sezione 5.8 a pagina 98) e le attività di protezione in tempo reale sulle workstation remote che fanno parte del gruppo di amministrazione.

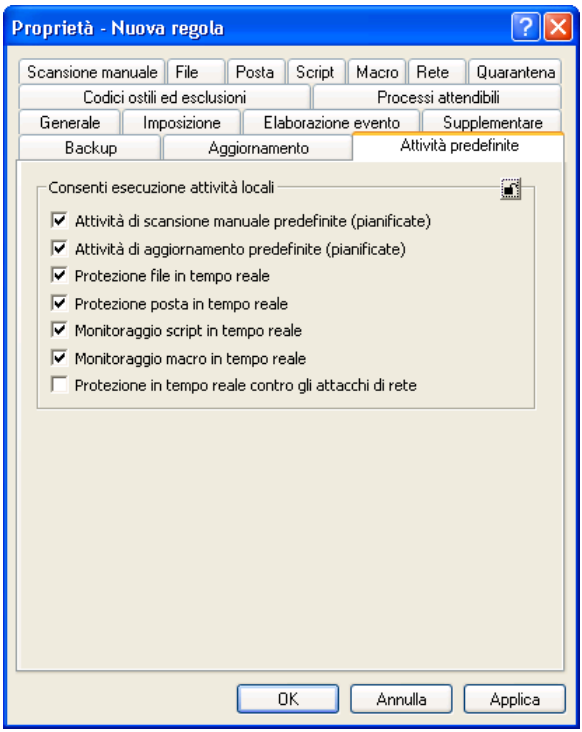

Figura 83. La scheda **Attività predefinite**

6.1.2.12. Configurazione dell'archiviazione in quarantena e nella memoria di backup

Le schede **Quarantena** (vedere la Figura 84) e **Backup** (vedere la Figura 85) consentono di specificare i parametri della regola per l'archiviazione in quarantena e nella memoria di backup.

Tali impostazioni sono analoghe a quelle dell'archiviazione in quarantena e nella memoria di backup gestita attraverso l'interfaccia locale (vedere la sezione 5.10.1.1 a pagina 103).

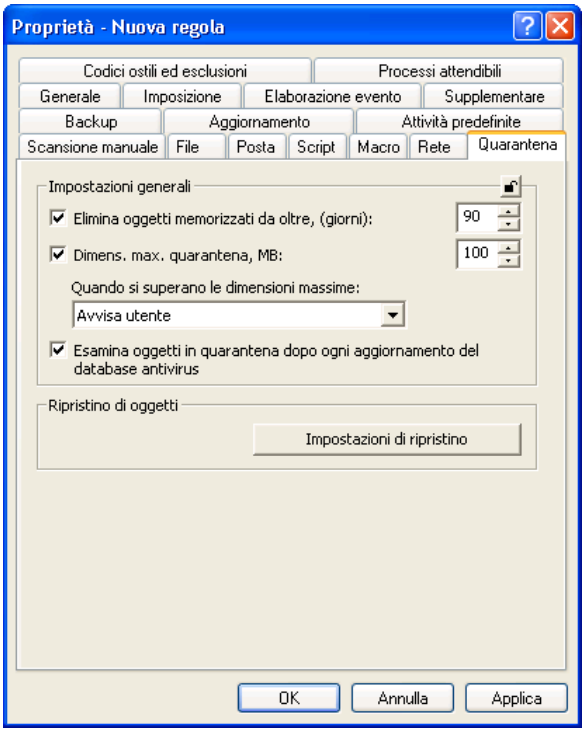

Figura 84. La scheda **Quarantena**

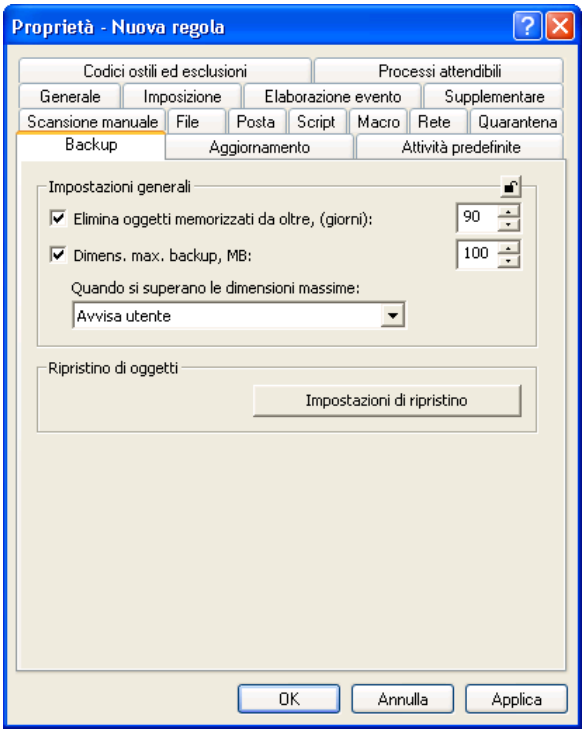

Figura 85. La scheda **Backup**

6.1.2.13. Generazione di report sul funzionamento dell'applicazione

La scheda **Elaborazione evento** (vedere la Figura 86) visualizza il tipo di eventi che si verificano durante il funzionamento dell'applicazione che vengono registrati nel report, oltre alla posizione del report e alle condizioni di notifica dell'amministratore e/o di altri utenti.

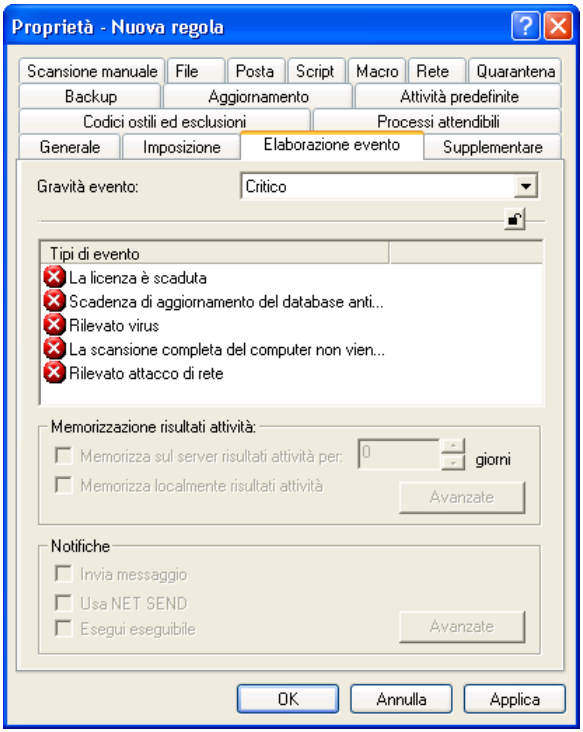

Figura 86. La scheda **Elaborazione evento**

Kaspersky Anti-Virus genera una serie di eventi verificatisi durante il funzionamento dell'applicazione. Ogni evento è accompagnato da uno stato di priorità. Esistono quattro stati di priorità possibili:

- **Evento critico**;
- **Errore**;
- **Avviso**;
- **Messaggio informativo**.

Agli eventi dello stesso tipo possono essere assegnati stati di priorità diversi, a seconda della situazione specifica.

Selezionare la priorità dell'evento dall'elenco a discesa **Gravità evento**. Il campo informativo sottostante visualizza i tipi di evento per il livello di priorità selezionato.

Tabella 2. Eventi dell'applicazione

Evento	Livello di importanza
Disinfettato oggetto	**Avviso**
Eliminato oggetto infetto	**Avviso**
Livello di protezione in tempo reale modificato	**Messaggio informativo**
La licenza sta per scadere (due settimane prima della data di scadenza)	**Avviso**
La licenza è scaduta	**Evento critico**
La licenza non ha superato la verifica	**Errore**
È stato rilevato un oggetto sospetto	**Avviso**
Errore di funzionamento	**Avviso** **Errore**
Scadenza di aggiornamento database antivirus superata – ritardo di una settimana (impossibile trovare) – ritardo di due settimane (impossibile trovare)	**Avviso** **Evento critico**
Rilevato virus	**Evento critico**
Rilevato attacco di rete	**Evento critico**
Errore interno	**Errore**
Il sistema operativo è stato riavviato	**Avviso**
L'applicazione è stata riavviata	**Avviso**

Evento	Livello di importanza
Rilevato archivio protetto da password	**Avviso**
Impossibile disinfettare l'oggetto	**Avviso**
La scansione completa del computer non viene eseguita da molto tempo: - da due settimane - da un mese	 **Avviso** **Evento critico**
Bloccato oggetto infetto	**Avviso**
Ignorato oggetto infetto	**Avviso**

* Questi valori sono quelli predefiniti. La finestra di dialogo **Notifiche** consente di modificarli (vedere la sezione 6.1.2.14 a pagina 150).

È possibile indicare se si desidera includere ogni evento nel report, nonché definire le impostazioni di notifica all'amministratore nel momento in cui l'evento si verifica.

Per una descrizione più dettagliata della scheda **Elaborazione evento**, consultare la guida dell'amministratore di Kaspersky Administration Kit 5.0.

6.1.2.14. Parametri supplementari

La scheda **Supplementare** (vedere la Figura 87) visualizza le impostazioni di assistenza di Kaspersky Anti-Virus 5.0 for Windows Workstations. La maggior parte di queste impostazioni è identica ai parametri supplementari descritti nella sezione 5.10.4 a pagina114.

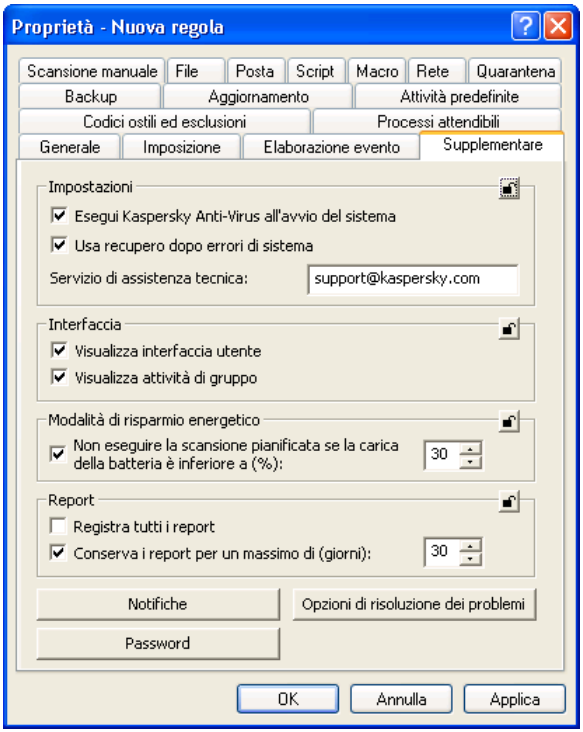

Figura 87. La scheda **Supplementare**

Facendo clic sul pulsante **Password** si apre una finestra che consente di impostare le seguenti password (vedere la figura 88):

- password per passare dalla modalità utente a quella amministratore (vedere la sezione 5.10.7 a pagina 120). Per abilitare questa modalità, selezionare la casella **Usa password di protezione applicazione**;
- è la password che verrà richiesta all'utente quando cerca di disinstallare Kaspersky Anti-Virus. Ciò impedisce la disinstallazione non autorizzata di Kaspersky Anti-Virus dalla workstation.

Figura 88. La finestra Password

La finestra che si apre facendo clic sul pulsante **Notifiche** (vedere la Figura 89) consente di impostare le condizioni per ricevere vari tipi di notifica:

- **Visualizza notifiche in caso di rilevamento di un oggetto pericoloso** - abilita la visualizzazione di messaggi che informano l'utente del rilevamento di un virus.
- **Visualizza messaggi informativi** - disabilita la visualizzazione dei messaggi di Kaspersky Anti-Virus
- **Usa animazione icona dell'aria di notifica** - abilita l'animazione dell'icona di Kaspersky Anti-Virus nell'area di notifica durante la scansione antivirus.
- **Abilita avvisi acustici** - consente l'emissione di segnali audio per notificare gli eventi che si verificano durante il funzionamento di Kaspersky Anti-Virus.

La sezione **Notifiche evento** consente di definire le impostazioni per ricevere le notifiche sullo stato dell'aggiornamento del database antivirus e la scansione completa del computer. Esistono due livelli per ciascuna di queste attività: un **avviso** e un **evento critico**.

Per ogni evento, è possibile impostare nel campo a destra il numero di giorni alla scadenza dei quali l'utente riceverà quotidianamente l'avviso corrispondente, all'avvio di Kaspersky Anti-Virus. Questo periodo ha inizio alla data dell'ultima esecuzione dell'attività corrispondente.

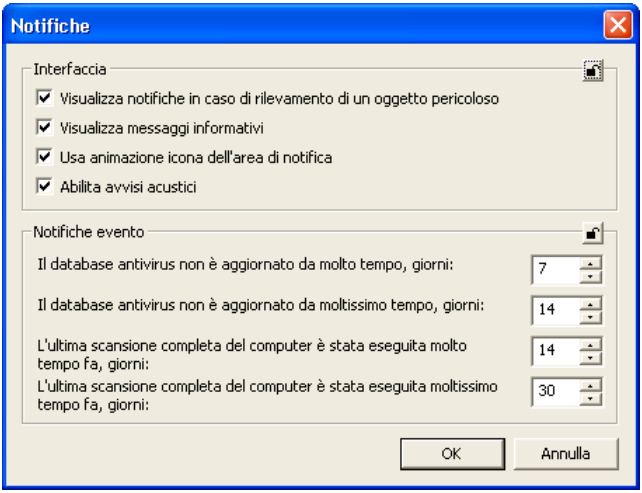
Notifiche
Interfaccia
Visualizza notifiche in caso di rilevamento di un oggetto pericoloso
Visualizza messaggi informativi
Usa animazione icona dell'area di notifica
Abilita avvisi acustici
Notifiche evento
Il database antivirus non è aggiornato da molto tempo, giorni:
7
Il database antivirus non è aggiornato da moltissimo tempo, giorni:
14
L'ultima scansione completa del computer è stata eseguita molto tempo fa, giorni:
14
L'ultima scansione completa del computer è stata eseguita moltissimo tempo fa, giorni:
30
OK
Annulla

Figura 89. La finestra **Notifiche**

Servirsi della finestra (vedere la figura 90) che si apre facendo clic sul pulsante **Opzioni di risoluzione dei problemi** (vedere v) per configurare i parametri che ottimizzano le prestazioni delle attività di scansione manuale. Le opzioni disponibili sono:

- **Disabilita la scansione degli account di posta durante l'esecuzione dell'attività** - disabilita la scansione della posta quando è in corso l'attività di scansione delle risorse del computer
- **Sospendi la scansione antivirus se il carico del sistema è superiore a (%)** - sospende la scansione antivirus se il carico del file system è superiore al livello specificato. Specificare il livello consentito di carico del sistema tramite un cursore o il campo d'immissione a destra dell'impostazione.

Opzioni di risoluzione dei problemi
Attività di scansione delle risorse del computer
Disabilita la scansione degli account di posta durante l'esecuzione dell'attività
Efficienza
Sospendi la scansione antivirus se il carico del sistema è superiore a (%)
30
OK
Annulla

Figura 90. La finestra **Opzioni di risoluzione dei problemi**

6.1.2.15. Visualizzazione dei risultati dell'applicazione delle regole

La scheda **Imposizione** (vedere la Figura 91) visualizza le seguenti informazioni sulla regola applicata ai computer del gruppo:

- Il numero di computer ai quali è stata assegnata la regola;
- Il numero dei computer ai quali è stata applicata la regola;
- Il numero dei computer per i quali l'applicazione della regola è in sospeso;
- Il numero dei computer per i quali l'applicazione della regola non è riuscita.

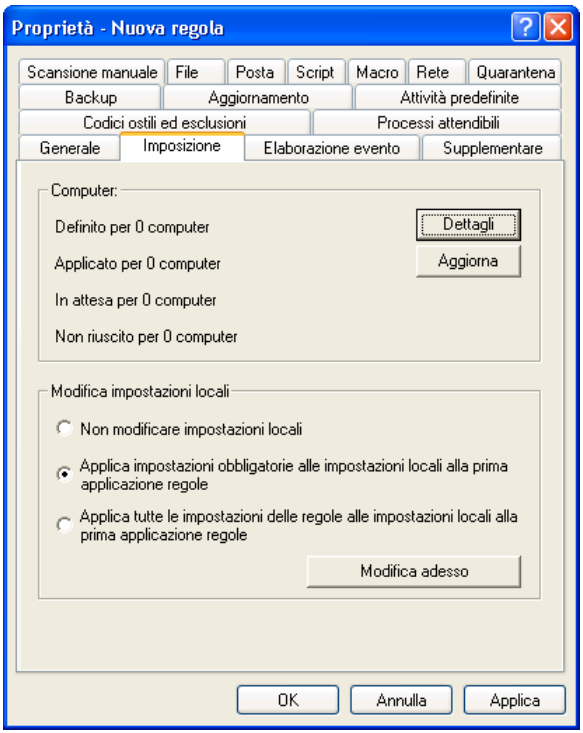

Figura 91. La scheda **Imposizione**

Fare clic su **Dettagli** per aprire una finestra di dialogo contenente dettagli sulla regola selezionata applicata a ciascun computer client. (per dettagli, vedere la guida di Kaspersky Administration Kit 5.0.)

La sezione **Modifica impostazioni locali** consente di specificare quali impostazioni saranno modificate nelle regole dei gruppi nidificati e nelle impostazioni dell'applicazione e delle attività sui computer client, la prima volta che verrà applicata la regola. È possibile selezionare una delle seguenti opzioni:

- **Non modificare impostazioni locali.** In questa caso, le impostazioni non saranno modificate.
- **Applica tutte le impostazioni delle regole alle impostazioni locali alla prima applicazione regole.** In questo caso, solo le impostazioni locali contrassegnate dall'icona verranno modificate. Per impedire che gli utenti possano modificare le impostazioni richieste sul computer client, fare clic su quest'icona. Essa passerà a .
- **Applica impostazioni obbligatorie alle impostazioni locali alla prima applicazione regole.** In questo caso, tutte le impostazioni locali verranno modificate secondo le impostazioni della regola. Come nel caso dell'opzione precedente, è possibile impedire agli utenti di modificare le impostazioni richieste.

Le impostazioni locali verranno modificate automaticamente alla prima applicazione della regola sul computer client. Per riapplicare la regola con le impostazioni modificate, premere il pulsante **Modifica adesso**.

6.2. Gestione delle attività

Questa sezione descrive le modalità di creazione e gestione delle attività di Kaspersky Anti-virus. Per istruzioni dettagliate sulla gestione delle regole, consultare la guida dell'amministratore di Kaspersky Administration Kit 5.0.

6.2.1. Creazione di un'attività

Durante l'installazione dell'applicazione, per ogni computer viene generato un elenco di attività di sistema. Tale elenco (vedere la Figura 92) comprende le attività di protezione in tempo reale (protezione del file system, protezione della posta elettronica, scansione delle macro e degli script), le attività di scansione manuale (scansione delle Risorse del computer, scansione automatica all'avvio di Kaspersky Anti-Virus, scansione della quarantena) e le attività di aggiornamento (aggiornamenti dei database antivirus, aggiornamenti dei moduli dell'applicazione, funzione di ripristino della versione precedente del database antivirus).

Le attività di protezione in tempo reale sono singole e vengono eseguite in background. Per le attività di scansione manuale e di aggiornamento dei database antivirus, è disponibile la pianificazione.

È possibile avviare le attività di sistema e modificarne i parametri e la pianificazione, ma non è possibile eliminarle.

Kaspersky Administration Kit consente di creare le seguenti attività per Kaspersky Anti-Virus:

- Attività locali assegnate a ciascun computer client;
- Attività di gruppo assegnate ai gruppi di computer client;
- Attività globali assegnate a un insieme di computer client da gruppi arbitrari su una rete logica.

È possibile modificare le impostazioni delle attività, controllarne l'esecuzione, copiare e spostare attività da un gruppo all'altro, ed eliminarle tramite i comandi del menu di scelta rapida standard, come **Copia/Incolla**, **Taglia/Incolla** e **Cancella**, o tramite comandi analoghi nel menu **Azione**.

I parametri dell'applicazione per ciascun computer client durante l'esecuzione di attività sono conformi alle regole del gruppo, alle impostazioni specifiche dell'attività e alle impostazioni dell'applicazione sul singolo computer client.

Tutte le attività sono pianificate per impostazione predefinita. Le attività possono essere temporaneamente escluse dall'elenco delle attività pianificate. In questo caso, non vengono eliminate dall'elenco delle attività: semplicemente, non vengono eseguite.

È possibile avviare, interrompere, terminare o riprendere manualmente un'attività per mezzo dei comandi **Avvia/Interrompi/Sospendi/Riprendi** nel menu di scelta rapida o nel menu **Azione**.

6.2.1.1. Creazione di un'attività locale

Per creare un'attività locale:

1. Nella cartella **Gruppi**, selezionare una cartella con il nome del gruppo cui appartiene il computer client.
2. Nella finestra dei risultati, selezionare il computer a cui si desidera assegnare la nuova attività locale e fare clic sul comando **Proprietà** nel menu di scelta rapida o nel menu **Azione**. Verrà visualizzata la finestra di dialogo **Proprietà <Nome computer>** con le proprietà del computer client (vedere la Figura 92).
3. Aprire la scheda **Attività** (vedere la Figura 92). Essa visualizza un elenco completo delle attività pianificate per questo computer

client.
Per creare una nuova attività locale, fare clic su **Aggiungi**. Fare clic su **Proprietà** per modificare le impostazioni dell'attività, e su **Elimina** per eliminare l'attività selezionata.

Fare clic su **Aggiungi** per creare una nuova attività. L'interfaccia dell'applicazione per la creazione di una nuova attività è organizzata come una procedura guidata di Windows, che segue l'utente durante la procedura. Per passare da una finestra all'altra della procedura guidata fare clic su **Indietro** e **Avanti**. Per terminare la procedura, fare clic su **Fine**. Per interrompere la procedura in qualsiasi momento, fare clic su **Annulla**.

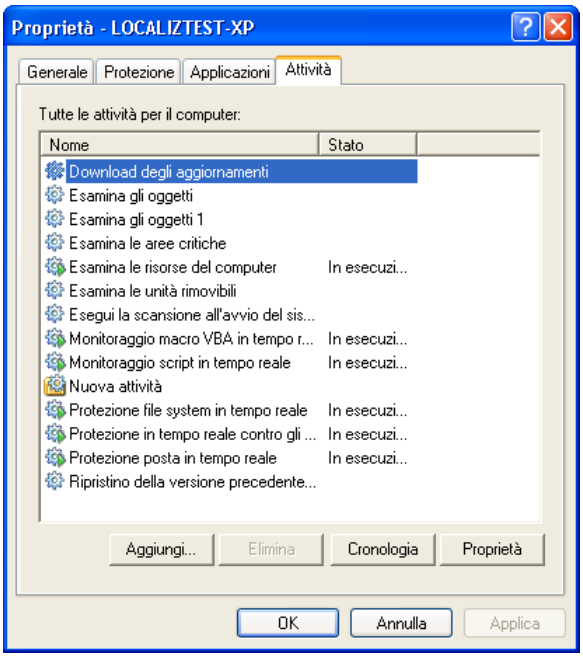

Figura 92. Creazione di un'attività locale
La scheda **Attività**

Fase 1. Informazioni generali sulla nuova attività

La prima finestra di dialogo della procedura guidata ha una funzione introduttiva: digitare qui il nome dell'attività (campo **Nome**).

Fase 2. Selezione dell'applicazione e il tipo di attività

Selezionare l'applicazione **Kaspersky Anti-Virus 5.0 for Windows Workstations** dall'elenco a discesa **Scegliere l'applicazione per cui definire un'attività**. Scegliere quindi il tipo di attività dall'elenco a discesa **Scegliere il tipo di attività da eseguire**. È possibile creare le seguenti attività per Kaspersky Anti-Virus:

- **Aggiorna database antivirus e moduli dell'applicazione** - aggiorna i database antivirus e i componenti dell'applicazione.
- **Ripristino vecchio database antivirus** - Ripristina versioni precedenti del database antivirus;
- **Scansione manuale** - avvia la scansione manuale di oggetti;
- **Installa chiave di licenza** - installa le chiavi di licenza.

Fase 3. Configurazione delle impostazioni per il tipo di attività selezionato

A seconda del tipo di attività selezionato, verranno proposte diverse opzioni per configurare le seguenti impostazioni di attività:

IMPOSTAZIONI DELL'ATTIVITÀ DI AGGIORNAMENTO DEL DATABASE ANTIVIRUS E DEI MODULI DELL'APPLICAZIONE

Le attività di aggiornamento dei database antivirus e dei moduli delle applicazioni sono configurate in maniera analoga alla creazione di una nuova regola (vedere gli Fase 4. - Fase 5. alle pagine 124-124). Inoltre, durante la creazione dell'attività è possibile definire, per esempio, i parametri di condivisione degli aggiornamenti ricevuti (vedere la sezione 5.1.3.2 a pagina 46).

CONGURAZIONE DELLE IMPOSTAZIONI DI RIPRISTINO DELLA VERSIONE PRECEDENTE DEL DATABASE

L'attività di ripristino di versioni precedenti del database antivirus non prevede impostazioni specifiche. Pertanto, una volta selezionata questa attività, la procedura guidata porta direttamente alla finestra di dialogo **Impostazioni di programmazione attività** (vedere la sezione 5.8 a pagina 98).

IMPOSTAZIONI DELL'ATTIVITÀ DI SCANSIONE MANUALE

Selezionare il livello di protezione predefinito per l'attività di scansione manuale (vedere la sezione 4.2 a pagina 36) e specificare l'azione da eseguire con l'oggetto nocivo rilevato (vedere la sezione 5.3.3.2 a pagina 82).

Facendo clic sul pulsante **Avanzate** si apre una finestra che consente di rivedere le impostazioni del livello di protezione antivirus selezionato ed eventualmente

personalizzarlo. In quest'ultimo caso, il livello di protezione passa allo stato **Personalizzato**.

Nella finestra di dialogo successiva (vedere la Figura 93), specificare gli oggetti da esaminare per mezzo dei pulsanti **Aggiungi, Modifica** e **Elimina**.

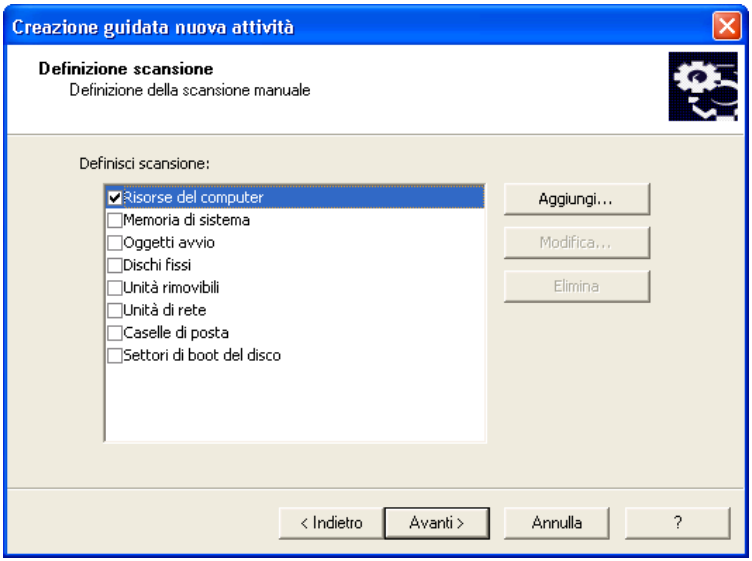

Figura 93. Elenco di oggetti da esaminare

IMPOSTAZIONI DELL'ATTIVITÀ DI INSTALLAZIONE DELLA CHIAVE DI LICENZA

Utilizzare il pulsante **Sfoglia** per individuare il percorso del file chiave. Per fare della chiave che si sta aggiungendo quella corrente, selezionare la casella **Usa come chiave licenza corrente**.

Non selezionare questa casella se si desidera aggiungere la chiave come riserva. Una chiave di riserva diventa la chiave corrente alla scadenza di quella precedentemente in uso.

Fase 4. Configurazione del lancio di un'attività per conto di un account utente selezionato

In questa fase (vedere la Figura 94) è possibile configurare l'avvio dell'attività creata per conto di un account utente in possesso di diritti di accesso sufficienti all'oggetto da esaminare o all'origine dell'aggiornamento (vedere il paragrafo 5.9 a pagina101).

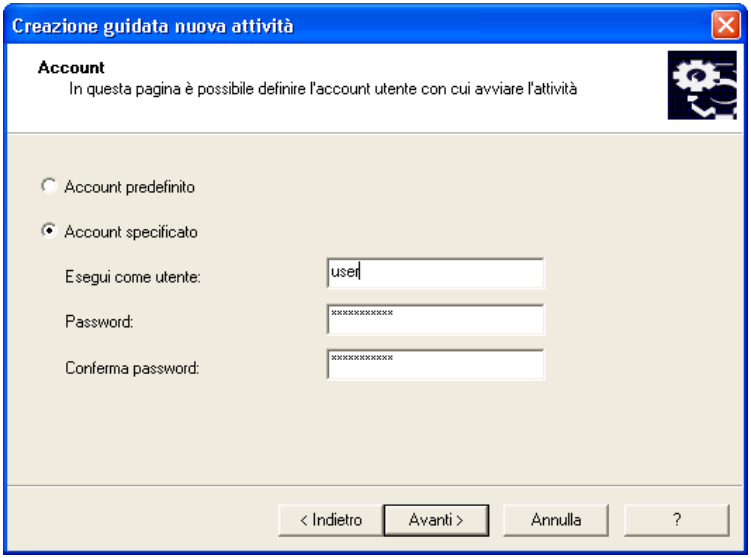

Figura 94. Configurazione dell'esecuzione di un'attività per conto di un altro account utente

Fase 5. Pianificazione

Dopo la configurazione delle attività selezionate, la procedura guidata apre la finestra di dialogo **Impostazioni di programmazione attività** (vedere la Figura 95), che consente di pianificare l'attività.

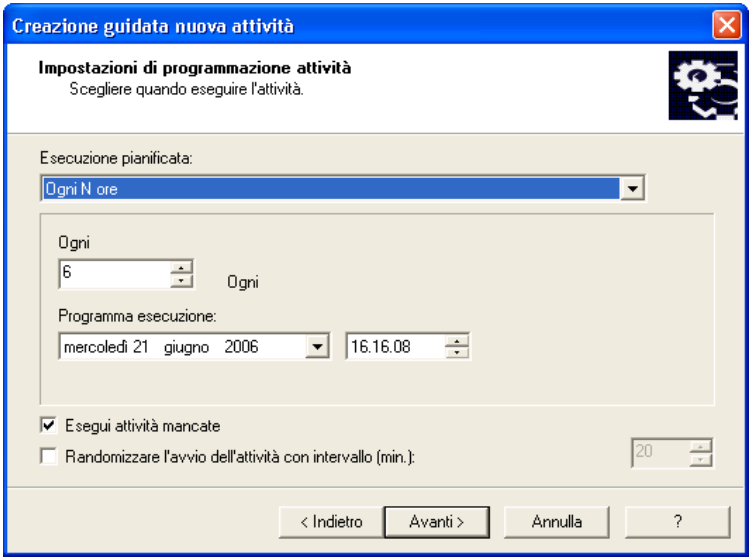

Figura 95. Pianificazione durante la creazione di una nuova attività

Selezionare la frequenza desiderata per l'attività dall'elenco a discesa **Esecuzione pianificata**. Sono disponibili le seguenti opzioni: *Ogni N ore, Ogni N giorni, Ogni N settimane, Manuale* e *All'avvio dell'applicazione*. In base alla selezione, gli elementi della finestra di dialogo cambiano:

Le attività di ripristino della versione precedente del database antivirus e di installazione della chiave di licenza possono essere avviate solo manualmente.

Per la pianificazione dell'avvio automatico delle attività, consultare la guida dell'amministratore di Kaspersky Administration Kit 5.0.

Fase 6. Completamento della creazione dell'attività

L'ultima finestra di dialogo della procedura guidata informa l'utente che l'attività è stata creata con successo.

6.2.1.2. Creazione di un'attività di gruppo

Per creare un'attività di gruppo per Kaspersky Anti-Virus:

1. Nella struttura ad albero della console, selezionare il gruppo di computer a cui applicare la nuova attività.
2. Selezionare la cartella **Attività** all'interno di questo gruppo, aprire il menu di scelta rapida e selezionare il comando **Nuovo/Attività**. Questo comando può essere selezionato anche dal menu **Azione**. Si avvia una procedura guidata per la creazione di una nuova attività di gruppo. La procedura è analoga a quella per la creazione di un'attività locale (vedere la sezione 6.2.1.1 a pagina 156).

La nuova attività creata sarà aggiunta alla cartella **Attività** del gruppo selezionato e di tutti i gruppi nidificati, e visualizzata nel pannello dei risultati.

6.2.1.3. Creazione di un'attività globale

Per creare un'attività globale per Kaspersky Anti-Virus:

1. Dalla struttura ad albero della consolle, selezionare il nodo **Attività globali**, aprire il menu di scelta rapida e selezionare il comando **Nuovo→Attività**. Questo comando può essere selezionato anche dal menu **Azione**.
2. Si avvia una procedura guidata per la creazione di una nuova attività globale. La procedura è analoga a quella per la creazione di un'attività locale (vedere la sezione 6.2.1.1 a pagina 156). L'unica differenza consiste nel fatto che l'utente deve definire un elenco di computer client sulla rete logica per l'attività globale.
3. Selezionare i computer desiderati nella rete logica a cui assegnare la nuova attività. È possibile selezionare computer da cartelle diverse o selezionare l'intera cartella (per ulteriori dettagli, consultare la guida dell'amministratore di Kaspersky Administration Kit 5.0).

Le attività globali vengono assegnate esclusivamente all'insieme di computer specificato. Per esempio, l'attività di installazione remota assegnata ad un gruppo non sarà eseguita sui nuovi computer client aggiunti al gruppo. A tal fine sarà necessario creare una nuova attività o modificare quella esistente come richiesto.

La nuova attività creata sarà aggiunta al nodo **Attività globali** della struttura ad albero della consolle, e visualizzata nel pannello dei risultati.

6.2.2. Visualizzazione e modifica delle impostazioni delle attività e monitoraggio del loro funzionamento

Per visualizzare e/o modificare le impostazioni delle attività:

- Nel caso di una attività locale, nella cartella **Gruppi**, selezionare la cartella con il nome del gruppo a cui appartiene il computer client. Nel pannello dei risultati, scegliere il computer desiderato e fare clic su **Proprietà** nel menu di scelta rapida. Si apre la finestra di dialogo **Proprietà - <nome computer>**. Passare alla scheda **Attività** (vedere la Figura 92). È possibile visualizzare e modificare le impostazioni delle attività selezionate nella finestra che si apre facendo clic sul pulsante **Proprietà**.

  La scheda **Attività** visualizza un elenco completo di attività assegnate al computer locale, che comprende sia le attività globali sia quelle di gruppo. Le attività locali e di gruppo sono contrassegnate da un'icona "cartella". Si noti che è possibile visualizzare le impostazioni di tutte le attività, ma solo quelle delle attività locali sono modificabili.

- Nel caso di una attività di gruppo, selezionare il gruppo desiderato nella struttura ad albero della consolle e scegliere la cartella **Attività** all'interno del gruppo scelto. Il pannello dei risultati visualizza tutte le attività assegnate al gruppo. Selezionare l'attività desiderata, aprire il menu di scelta rapida e fare clic su **Proprietà** (oppure selezionare **Proprietà** nel menu **Azione**).

- Per modificare le impostazioni delle attività globali, selezionare il nodo **Attività** nella struttura ad albero della consolle, scegliere l'attività desiderata, aprire il menu di scelta rapida e fare clic su **Proprietà** (oppure selezionare **Proprietà** nel menu **Azione**).

Si apre la finestra di dialogo **Proprietà: Nome attività**, composta dalle seguenti schede: **Generale**, **Impostazioni**, **Account, Pianifica**, e **Notifiche**. La finestra di dialogo di configurazione dell'attività globale contiene la scheda supplementare **Computer target** per i quali viene creata l'attività.

Tutte le schede (ad eccezione delle schede **Impostazioni** e **Account**) sono schede standard di Kaspersky Administration Kit 5.0. Per ulteriori informazioni su queste schede consultare la guida dell'amministratore di Kaspersky Administration Kit. La scheda **Impostazioni** visualizza impostazioni specifiche di Kaspersky Anti-Virus, a seconda del tipo di attività selezionata (vedere il Fase 3. a pagina 158). La scheda **Account** consente di configurare il lancio dell'attività per conto dell'account (vedere la sezione 5.9 a pagina 101).

6.2.3. Esecuzione e interruzione delle attività

Le attività del computer possono essere avviate solo se l'applicazione corrispondente è in esecuzione. Se l'applicazione viene chiusa, vengono interrotte anche tutte le attività in esecuzione.

Tutte le attività possono essere eseguite e interrotte automaticamente, in base agli orari programmati, o manualmente, per mezzo delle opzioni del menu di scelta rapida o dalla finestra di visualizzazione delle impostazioni. È possibile anche interrompere un'attività e riprenderla in seguito.

Per avviare/interrompere/sospendere/riprendere manualmente un'attività:

selezionare l'attività desiderata, aprire il menu di scelta rapida e selezionare il comando **Avvia/Interrompi/Sospendi/Riprendi** nel menu stesso o dal menu **Azione**.

Comandi simili sono accessibili anche dalla finestra di configurazione delle attività, tramite i pulsanti corrispondenti nella scheda **Generale** (vedere la sezione 6.2.2 a pagina 163).

6.3. Configurazione delle impostazioni dell'applicazione

È possibile modificare i parametri dell'applicazione per i singoli computer client di un gruppo. Possono essere modificate solo le impostazioni definite modificabili in base alla regola dell'applicazione.

Per modificare le impostazioni dell'applicazione:

1. Nella cartella **Gruppi**, selezionare la cartella con il nome del gruppo cui appartiene il computer client.
2. Nella finestra dei risultati, selezionare il computer per il quale si desidera modificare le impostazioni dell'applicazione e fare clic sul comando **Proprietà** nel menu di scelta rapida o nel menu **Azione**.
3. In seguito a questa azione, nella finestra principale del programma si apre la finestra di dialogo **Proprietà - <Nome computer>**, composta da quattro schede. Selezionare la scheda **Applicazioni** (vedere la Figura 96) che visualizza un elenco completo delle applicazioni Kaspersky Lab installate sul computer client.
4. Selezionare **Kaspersky Anti-Virus 5.0 for Windows Workstations**. Sotto all'elenco, sono visibili i pulsanti **Eventi**, **Statistiche**, e **Proprietà** che consentono di:
   - Visualizzare un elenco degli eventi verificatisi nel computer client connesso al server di amministrazione (per ulteriori informazioni sui report, vedere la guida dell'amministratore di Kaspersky Administration Kit 5.0).
   - Visualizzare le statistiche correnti sul funzionamento dell'applicazione.
   - Accedere alle impostazioni dell'applicazione. Facendo clic sul pulsante si apre una finestra che contiene le seguenti schede: **Generale**, **Supplementare**, Codici ostili ed esclusioni, Processi attendibili, Programmi potenzialmente pericolosi, **Quarantena**, **Backup**, **Oggetti in memoria**, **Licenze**, e **Elaborazione evento**. Per una descrizione dettagliata delle schede leggere le sezioni successive.

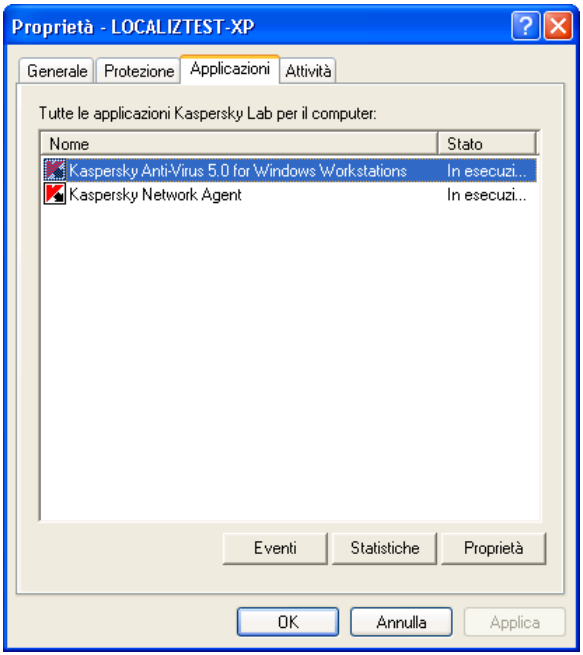

Figura 96. Finestra di dialogo delle proprietà del computer client
La scheda **Applicazioni**

6.3.1. Visualizzazione delle informazioni sull'applicazione

La scheda **Generale** (vedere la Figura 97) consente di esaminare le informazioni generali sull'applicazione (Kaspersky Anti-Virus 5.0 for Windows Workstations) e di avviarne o interromperne il funzionamento.

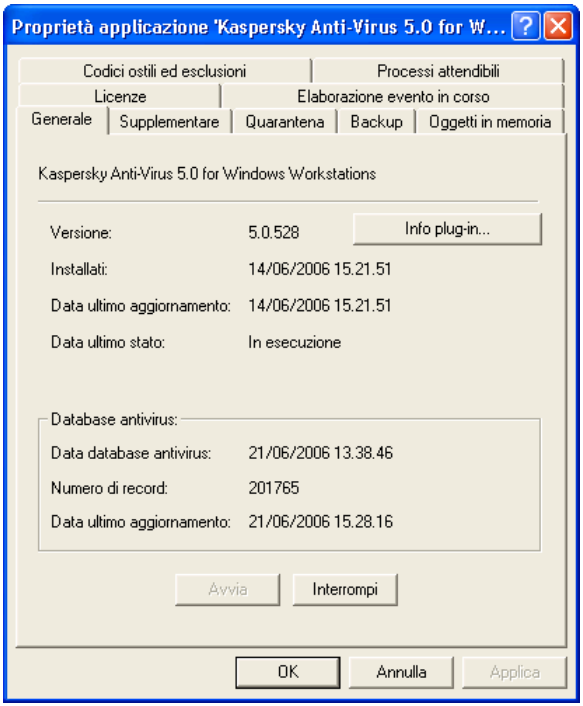

Figura 97. Finestra Proprietà applicazione. La scheda **Generale**

La sezione superiore della finestra visualizza il titolo dell'applicazione installata, la versione, la data di installazione, lo stato (se l'applicazione è in esecuzione oppure no su un computer locale) nonché le informazioni relative alle condizioni dei database antivirus.

Per avviare/interrompere l'applicazione, utilizzare i pulsanti corrispondenti.

Il pulsante **Info plug-in** consente di visualizzare informazioni generali sul plug-in di amministrazione per Kaspersky Anti-Virus 5.0 for Windows Workstation (vedere la Figura 98).

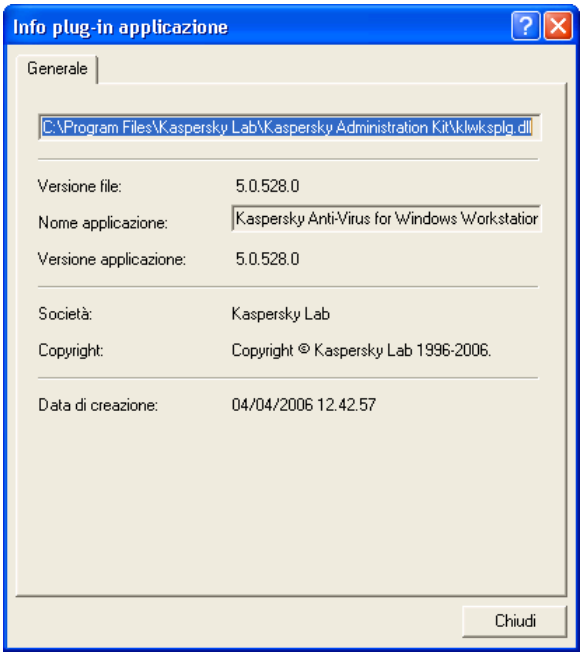

Figura 98. Informazioni sul plug-in di amministrazione dell'applicazione

6.3.2. Impostazioni supplementari dell'applicazione

Le schede **Supplementare**, **Quarantena, Riskware, Processi attendibili** e **Backup** consentono di impostare i parametri di Kaspersky Anti-Virus su una workstation remota.

Queste impostazioni replicano quelle delle regole di gruppo corrispondenti (per ulteriori dettagli, vedere la sezione 6.1.2 a pagina 126). Le impostazioni delle regole restano predominanti ai fini della configurazione dell'applicazione.

Durante la configurazione delle impostazioni dell'applicazione in un computer locale, è possibile modificare solo i parametri la cui modifica è consentita dalla regola di gruppo.

6.3.3. Uso delle aree di archiviazione di quarantena e backup

Kaspersky Anti-Virus salva gli oggetti sospetti e le copie di backup dei file in apposite aree di archiviazione.

Ogni computer ha le proprie cartelle di archiviazione per quarantena e backup.

È possibile visualizzare un elenco degli oggetti in quarantena o delle copie di backup su un computer dalla scheda **Oggetti in memoria** (vedere la Figura 99).

Per fare ciò, fare clic sul pulsante **Elenco di oggetti** nella sezione **Quarantena** o **Memoria di backup** rispettivamente.

Se l'applicazione non è in grado di stabilire la connessione con il computer client, verrà visualizzata una finestra di dialogo da cui è possibile riprovare o annullare il tentativo.

Le finestre di dialogo che visualizzano il contenuto di entrambe le aree di memorizzazione sono analoghe (vedere la Figura 100). Nella sezione centrale della finestra di dialogo è visibile un elenco dei file in quarantena o delle copie di backup. Per ogni oggetto sono fornite le seguenti informazioni: nome, stato, data del trasferimento in quarantena e percorso originale dell'oggetto.

Al di sopra dell'elenco si trova una barra degli strumenti per la gestione degli oggetti in quarantena o delle copie di backup. Servirsi dei seguenti pulsanti per:

- Ripristinare un oggetto. Fare clic su questo pulsante per ripristinare l'oggetto, specificando il percorso desiderato.

  Nel caso di una gestione remota tramite Kaspersky Administration Kit, gli oggetti possono essere ripristinati solo su un computer in cui sia installata la *Consolle di amministrazione*.

- Eliminare l'oggetto dalla cartella di archiviazione.
- Aggiornare il contenuto dell'archiviazione.
- Effettuare una nuova scansione degli oggetti (solo per la quarantena).

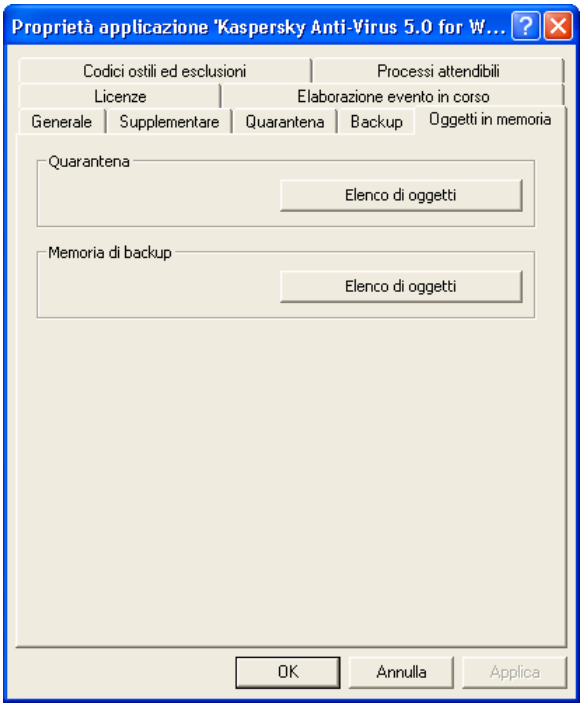

Figura 99. La scheda **Oggetti in memoria**

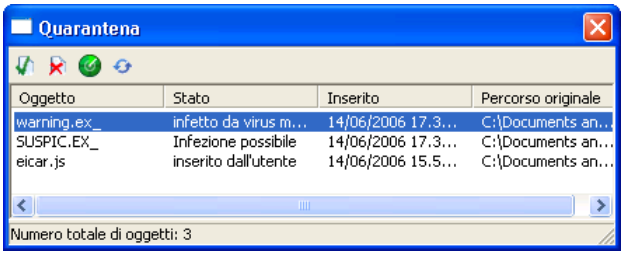

Figura 100. Archiviazione in quarantena

6.3.4. Visualizzazione delle informazioni sulle chiavi di licenza

La scheda **Licenze** (vedere la Figura 101) ha fini puramente informativi. Essa visualizza le informazioni sulle chiavi di licenza correnti e di riserva installate su un computer specifico.

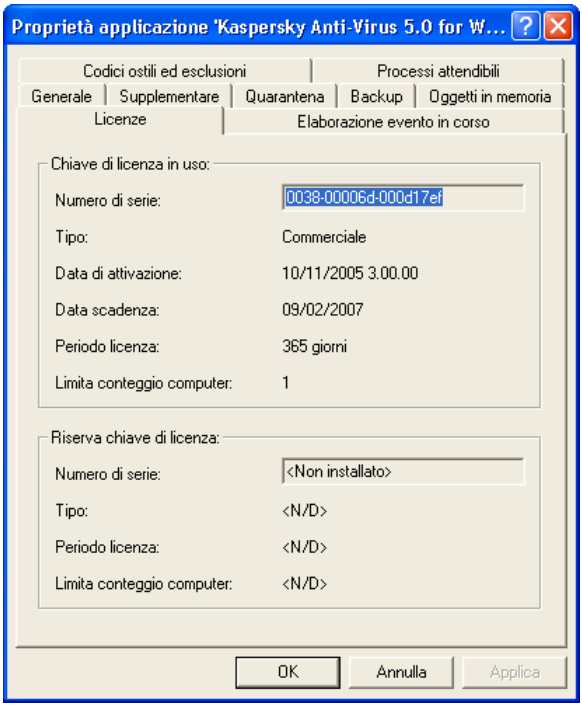

Figura 101. La scheda **Licenze**

6.3.5. Configurazione dei parametri per la generazione dei report

La scheda **Elaborazione evento** consente di accedere ai parametri del servizio di comunicazione, che invia informazioni sul funzionamento dell'antivirus da un computer remoto.

Essa replica i parametri della corrispondente scheda delle regole di gruppo (vedere la sezione 6.1.2.13 a pagina 147).

CAPITOLO 7. TEST DI FUNZIONAMENTO DI KASPERSKY ANTI-VIRUS

7.1. "Virus" di prova EICAR e sue modifiche

Dopo aver installato e personalizzato Kaspersky Anti-Virus, si consiglia di testare l'efficacia delle impostazioni e del funzionamento dell'applicazione servendosi di un “virus” di prova o di una sua modifica.

Il virus di prova è stato progettato specificamente dall'organizzazione eicar (l'European Institute for Computer Antivirus Research) per il collaudo dei prodotti antivirus.

NON SI TRATTA DI UN VERO E PROPRIO VIRUS, poiché non contiene codici in grado di danneggiare realmente il computer. Ciononostante, la maggior parte dei prodotti antivirus lo identifica come tale.

Non usare mai virus autentici per testare il funzionamento di un programma antivirus!

Il "virus" di prova può essere scaricato dal sito web ufficiale di **EICAR** all'indirizzo http://www.eicar.org/anti_virus_test_file.htm. Se non si dispone di connessione Internet, è possibile creare personalmente un "virus" di prova. Per fare ciò, digitare la seguente stringa in qualsiasi editor di testo e salvare il file come **eicar.com**:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

Il file scaricato dal sito web di **EICAR** o creato secondo quanto descritto sopra contiene il corpo di un "virus" di prova standard. Kaspersky Anti-Virus lo rileverà e lo assegnerà alla categoria **Infetto**, applicando l'azione specificata dall'amministratore per gli oggetti di questo tipo.

Per verificare la reazione dell'applicazione antivirus ad altri tipi di oggetto, modificare il corpo di questo "virus" di prova standard aggiungendo uno dei prefissi elencati nella Tabella Tabella3.

È possibile verificare il corretto funzionamento di Kaspersky Anti-Virus tramite il "virus" modificato EICAR solo se il database antivirus utilizzato è stato aggiornato il 24 ottobre 2003 o in data successiva, o dispone degli aggiornamenti cumulativi per Ottobre 2003.

Tabella3. Varianti del "virus" di prova

Prefisso	Tipo di oggetto
Nessun prefisso, "virus" di prova standard	**Infetto** - Si verifica un errore durante il tentativo di disinfettare l'oggetto; esso viene eliminato.
CORR–	**Corrotto**
SUSP–	**Sospetto** (codice virale ignoto)
WARN–	**Attenzione** (codice modificato di virus conosciuto)
ERRO–	**Errore durante la scansione dell'oggetto**
CURE–	**Infetto** - L'oggetto viene disinfettato; il testo del "virus" di prova viene modificato in CURE
DELE–	**Infetto** – L'oggetto viene eliminato automaticamente

La prima colonna della tabella elenca i prefissi da aggiungere all'inizio della stringa del "virus" di prova standard (ad esempio, DELE–X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*).

Dopo aver aggiunto un prefisso al "virus" di prova, salvarlo, ad esempio, in un file con il nome eicar_dele.com; chiamare in maniera analoga le altre varianti del "virus" di prova.

La seconda colonna di questa tabella contiene i tipi di oggetto identificati dall'applicazione antivirus dopo l'aggiunta di un prefisso. Le azioni applicate a ciascun tipo di oggetto sono definite in base alle impostazioni dell'applicazione Kaspersky Anti-Virus personalizzate dall'amministratore.

7.2. Prova del corretto funzionamento di Kaspersky Anti-Virus

Per verificare il corretto funzionamento di Kaspersky Anti-Virus 5.0 for Windows Workstation e l'efficacia delle sue impostazioni:

- Creare una directory sul disco e salvare in essa i "virus" di prova creati.
- Creare un'attività utente personalizzata e definirne i parametri (vedere la sezione 5.6 a pagina 93):
  - aggiungere la cartella contenente i "virus" di prova creati all'elenco degli oggetti da esaminare all'esecuzione dell'applicazione;
  - Selezionare l'opzione *Richiedi intervento utente durante la scansione* come azione da eseguire al rilevamento di oggetti infetti o sospetti da parte di Kaspersky Anti-Virus.
- Nella finestra di dialogo **Impostazioni supplementari** (vedere la sezione 5.10.4 a pagina 114), selezionare la casella **Registra tutti i messaggi** per salvare i dati sugli oggetti corrotti o sugli oggetti che non è stato possibile esaminare a causa di errori.
- Eseguire l'attività.

Durante la procedura di scansione, non appena vengono rilevati oggetti sospetti o infetti, l'applicazione visualizza una finestra di dialogo contenente informazioni su tali oggetti e chiede all'utente di selezionare l'azione desiderata. Per esempio, se viene rilevato un oggetto con prefisso SUSP-, viene visualizzato il seguente messaggio:

Kaspersky Anti-Virus for Windows Workstations
Attenzione! Rilevato un oggetto sospetto.
Oggetto: file C:\eicar\eicar.com.suspicious
Conclusione: Forse è infettato da virus EICAR-Test-File.
Si raccomanda di mettere in quarantena l'oggetto.
Isola (raccomandato)
Elimina
Ignora
Applica a tutti sospetti oggetti che non possono essere disinfettati (in questa sessione)
OK

Figura 102. Attenzione! Rilevato oggetto sospetto

In tal modo è possibile verificare la reazione dell'applicazione alla scoperta di oggetti di diversi tipi selezionando varie opzioni nelle finestre di dialogo visualizzate durante la scansione.

Il report conterrà una sintesi completa dei risultati della scansione (vedere la Figura 103).

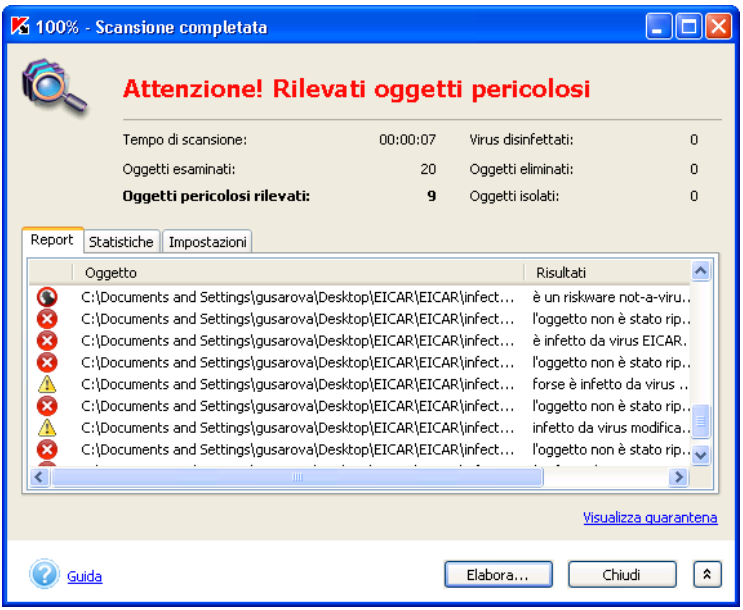
100% - Scansione completata
Attenzione! Rilevati oggetti pericolosi
Tempo di scansione: 00:00:07
Oggetti esaminati: 20
Oggetti pericolosi rilevati: 9
Virus disinfettati: 0
Oggetti eliminati: 0
Oggetti isolati: 0
Report
Statistiche
Impostazioni
Oggetto
Risultati
C:\Documents and Settings\gusarova\Desktop\EICAR\EICAR\infect... è un riskware not-a-viru..
C:\Documents and Settings\gusarova\Desktop\EICAR\EICAR\infect... l'oggetto non è stato rip..
C:\Documents and Settings\gusarova\Desktop\EICAR\EICAR\infect... è infetto da virus EICAR.
C:\Documents and Settings\gusarova\Desktop\EICAR\EICAR\infect... l'oggetto non è stato rip..
C:\Documents and Settings\gusarova\Desktop\EICAR\EICAR\infect... forse è infetto da virus ..
C:\Documents and Settings\gusarova\Desktop\EICAR\EICAR\infect... l'oggetto non è stato rip..
C:\Documents and Settings\gusarova\Desktop\EICAR\EICAR\infect... infetto da virus modifica..
C:\Documents and Settings\gusarova\Desktop\EICAR\EICAR\infect... l'oggetto non è stato rip..
Visualizza quarantena
Guida
Elabora...
Chiudi

Figura 103. Il report della scansione della cartella contenente i "virus" di prova

CAPITOLO 8. GESTIONE DELLE CHIAVI DI LICENZA

È possibile utilizzare Kaspersky Anti-Virus solo dopo aver installato la chiave di licenza compresa nel kit di installazione del prodotto.

Senza la chiave di licenza Kaspersky Anti-Virus NON funziona!

Alla scadenza della licenza, la funzionalità di Kaspersky Anti-Virus rimane immutata, ma non sarà possibile aggiornare il database antivirus. Restano possibili la scansione del computer e della posta elettronica e la disinfezione degli oggetti infetti rilevati, ma solo utilizzando i vecchi database antivirus aggiornati alla data di scadenza della licenza. Per questo motivo, non è garantita la protezione del computer dai nuovi virus che possono diffondersi dopo la scadenza della licenza per Kaspersky Anti-Virus.

Per evitare il rischio di infezione del computer da parte di nuovi virus, è consigliabile rinnovare la licenza per Kaspersky Anti-Virus.

Due settimane prima della scadenza della licenza, Kaspersky Anti-Virus visualizzerà una notifica. Per due settimane, sarà visualizzato un messaggio di avviso ogni volta che viene avviata l'applicazione.

Per rinnovare la licenza è necessario acquistare e installare una nuova chiave di licenza per Kaspersky Anti-Virus. Per fare ciò:

1. Rivolgersi al rivenditore presso il quale si è acquistato il prodotto e acquistare una nuova chiave di licenza per Kaspersky Anti-Virus 5.0 for Windows Workstations;

oppure:

acquistare la chiave di licenza direttamente da Kaspersky Lab seguendo il collegamento Rinnovo licenza nella scheda **Assistenza** (vedere la figura 4), oppure scegliendo il pulsante **Rinnova** nella finestra **Gestione delle chiavi di licenza** (vedere la Figura 104). Compilare il modulo sulla pagina del nostro sito Web che si aprirà. Dopo il pagamento, si riceverà un collegamento sull'indirizzo di posta elettronica specificato nel modulo d'ordine. Seguire questo collegamento per scaricare la chiave di licenza.

Kaspersky Lab annuncia periodicamente offerte speciali che consentono di godere di notevoli sconti quando si rinnova la licenza per l'utilizzo dei nostri prodotti. Per avere informazioni sulle nostre offerte, visitare il sito Web di Kaspersky Lab alle sezioni **Products → Sales and special offers**.

2. Installare la chiave di licenza. Per una descrizione dettagliata su come gestire la chiave di licenza tramite l'apposita interfaccia locale, vedere la sezione 8.1 a pagina 177; per una descrizione dettagliata sull'uso dell'interfaccia di Kaspersky Administration Kit, vedere la sezione 8.2 a pagina 180.

È possibile installare due chiavi: una chiave corrente e una di riserva. La chiave corrente è la chiave attualmente utilizzata dall'applicazione. Non è possibile installare più di una chiave con lo stato “corrente”. La chiave di riserva sarà attivata alla scadenza di quella corrente.

8.1. Gestione delle chiavi utilizzando l'interfaccia locale

Per rinnovare la chiave di licenza tramite l'interfaccia locale di Kaspersky Anti-Virus for Windows Workstations:

1. Acquistare una chiave di licenza (per dettagli, vedere le pagine precedenti).
2. Installare la chiave di licenza. Per fare ciò:
   a. Seguire il collegamento Chiavi di licenza nella sezione sinistra della scheda **Assistenza** (vedere la figura 4).
   b. Nella finestra **Gestione delle chiavi di licenza** (vedere la Figura 104), scegliere il pulsante **Aggiungi**.
   c. Tramite la finestra di dialogo standard per la selezione dei file, passare alla cartella in cui si trova la chiave di licenza (file con estensione **.key**). Selezionare la chiave di licenza desiderata e scegliere il pulsante **Apri**.
   d. Leggere le informazioni relative alla chiave che si sta aggiungendo nella finestra **Attivazione della chiave di licenza** che verrà visualizzata (vedere la figura 105) e scegliere il pulsante **Attiva** per iniziare a utilizzare questa chiave.

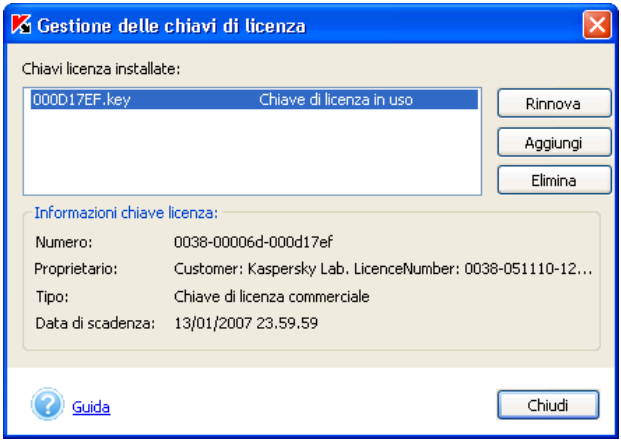

Figura 104. Finestra di gestione delle chiavi di licenza

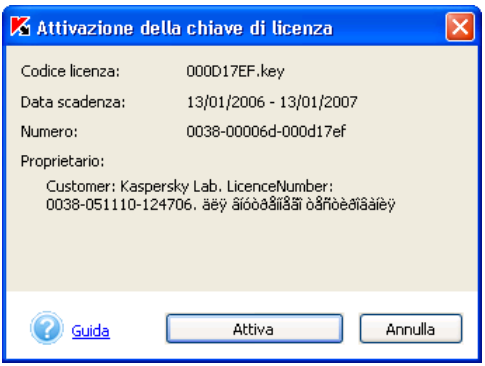

Figura 105. Finestra Attivazione della chiave di licenza

oppure:

a. Selezionare il gruppo Kaspersky Anti-Virus dal menu **Start** → **Tutti i programmi** e selezionare la voce **Installare la chiave di licenza**.

b. Scegliere il pulsante **Sfoglia** nella finestra che verrà visualizzata e selezionare la cartella in cui si trova il file della chiave di licenza.

c. Selezionare la chiave di licenza desiderata e scegliere il pulsante **Apri**.

d. Nella parte inferiore della finestra di dialogo (vedere la Figura 106), selezionare la casella accanto al nome dell'applicazione

per la quale installare la chiave di licenza. Scegliere il pulsante **OK**.

Se l'elenco nella parte inferiore della finestra di dialogo e vuoto, ciò significa che la chiave di licenza non è idonea alle applicazioni di Kaspersky Lab installate sul computer.

Selezionare un altro file della chiave di licenza.

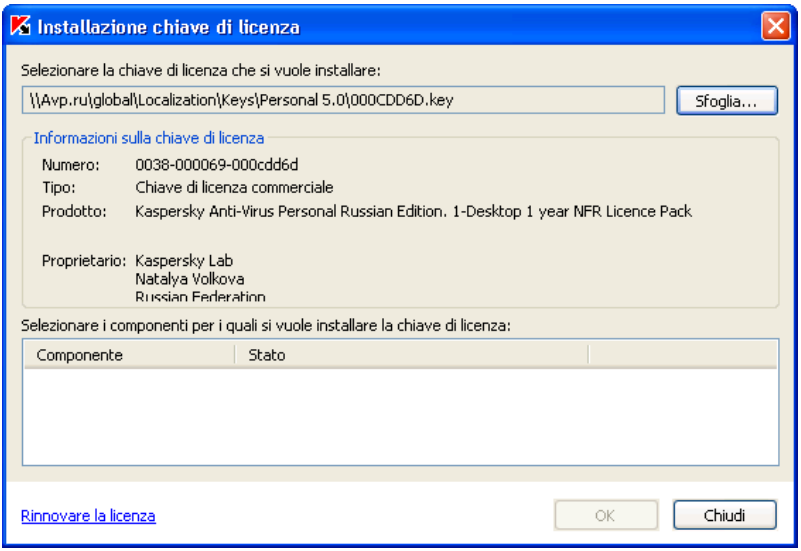

Figura 106. La finestra di dialogo **Installazione chiave di licenza**.

e. Rivedere le informazioni relative alla chiave che si sta aggiungendo nella finestra di dialogo **Attivazione chiave di licenza** che verrà visualizzata (vedere la Figura 105), quindi scegliere il pulsante **Attiva** per iniziare ad utilizzare la chiave.

Se si sta aggiungendo una nuova chiave mentre la chiave corrente ancora valida, verranno proposte due opzioni di installazione della chiave:

- È possibile aggiungere la chiave come chiave di riserva (raccomandato). Se si seleziona questa opzione, la chiave verrà aggiunta all'elenco come *chiave di riserva*. Una volta scaduta la chiave corrente, tale nuova chiave diventerà automaticamente quella *corrente*.
- Sostituire la chiave di licenza corrente con la nuova. Se si seleziona questa opzione, la nuova chiave verrà aggiunta all'elenco come chiave *corrente*.

Si noti che, se si elimina la chiave corrente, verrà eliminata automaticamente anche la chiave di riserva installata!

8.2. Gestione delle chiavi di licenza tramite l'interfaccia di Kaspersky Administration Kit

Se il pacchetto è controllato tramite Kaspersky Administration Kit, è possibile rinnovare una licenza in base a uno dei seguenti due metodi:

- *Aggiunta licenza gruppo* estende simultaneamente la licenza per Kaspersky Anti-Virus di computer o gruppi di computer client selezionati tramite le attività globali o di gruppo (per dettagli, vedere la guida dell'amministratore di Kaspersky Administration Kit 5.0).
- *Aggiunta di licenza singola* estende la licenza per Kaspersky Anti-Virus di un solo computer.

Per rinnovare la licenza per una workstation è necessario acquistare ed installare una nuova chiave di licenza per Kaspersky Anti-Virus. Per fare ciò:

1. Acquistare una chiave di licenza (vedere la Capitolo 8 a pagina 176).
2. Creare un'attività locale per l'installazione della chiave di licenza (vedere la sezione 6.2.1.1 a pagina 156).

È possibile rivedere le informazioni sulle chiavi di licenza (corrente e di riserva) installate su un computer specifico tramite la scheda **Licenze** (vedere la sezione 6.3.4 a pagina 171).

CAPITOLO 9. GESTIONE DELL'APPLICAZIONE DALLA RIGA DI COMANDO

Kaspersky Anti-Virus può essere gestito dalla riga di comando utilizzando l'utility **kavshell.exe** inclusa nel pacchetto di distribuzione. Dopo l'installazione di Kaspersky Anti-Virus, questa utility è ubicata nella cartella root di installazione dell'applicazione. Quando si avvia questa utility dalla riga di comando, a seconda dei comandi utilizzati saranno disponibili le seguenti funzioni:

SCAN	Scansione degli oggetti selezionati
FULLSCAN	Scansione completa del computer
UPDATE	Aggiornamento del database anti-virus e dei moduli dell'applicazione
ROLLBACK	Ripristino della versione precedente del database antivirus
RTP	Gestione della modalità di protezione del computer in tempo reale
START	Avvio di Kaspersky Anti-Virus
STOP	Arresto di Kaspersky Anti-Virus
TASK	Gestione delle attività di Kaspersky Anti-Virus
IMPORT	Importazione delle impostazioni di Kaspersky Anti-Virus da un file
EXPORT	Esportazione delle impostazioni di Kaspersky Anti-Virus in un file

ADDKEY	Aggiunta di una chiave di licenza

Se l'utilizzo delle modalità utente e amministratore è abilitato nelle impostazione di Kaspersky Anti-Virus (vedere la sezione 5.10.7 a pagina 120), alcuni comandi saranno disponibili esclusivamente per gli amministratori dell'applicazione.

Per visualizzare la sintassi dei comandi utilizzare:

```
KAVSHELL HELP [command] [3]
KAVSHELL [command] /?
```

Se il modificatore **tasto** non viene specificato, verrà visualizzato un elenco di tutti i comandi disponibili

Esempi:

```
KAVSHELL HELP SCAN
KAVSHELL SCAN /?
```

9.1. Scansione degli oggetti selezionati

Sintassi del comando:

KAVSHELL SCAN [objects] [/L[!]:objects_file] [/F(A|E|C)] [/DISINFECT|/DELETE] [/W[A][!]:report_file]

Se non vengono specificati i modificatori, verrà visualizzata la guida relativa alla sintassi del comando.

Le attività di scansione verranno eseguite con le impostazioni raccomandate dagli esperti di Kaspersky Lab.

Oggetti	Crea l'elenco comprendendo uno o più file, cartelle od oggetti predefiniti, separati da uno spazio: Tipi di oggetti predefiniti:

[3] I tasti opzionali sono visualizzati tra parentesi quadre.

	• **/MEMORY** - memoria di sistema; • **/STARTUP** - oggetti di avvio; • **/MAIL** - caselle di posta di Microsoft Outlook e Microsoft Outlook Express; • **/REMDRIVES** - unità rimovibili; • **/FIXDRIVES** - unità di sistema; • **/NETDRIVES** - unità di rete. Commenti: • Se il nome di un oggetto contiene uno spazio, deve essere digitato tra virgolette; • se si desidera eseguire la scansione di diversi file, è possibile utilizzare le maschere (gli esempi di maschere sono disponibili nella sezione 5.7 a pagina 94); • se se viene specificata una cartella specifica, verranno esaminati tutti i file in essa contenuti.
/L[!]:objects_file	Crea un file in formato .txt contenente l'elenco di oggetti da esaminare (file, cartelle, oggetti predefiniti). Il nome di ciascun oggetto nel file deve iniziare su una nuova riga. Il simbolo ! viene utilizzato per cancellare il file degli oggetti una volta terminata la scansione. È possibile utilizzare percorsi assoluti o relativi al file. Se il percorso contiene spazi, dev'essere digitato tra virgolette.
/F(A|E|C) **/FA** **/FC** **/FE**	Tipi di file da esaminare: • esamina tutti i file. • esamina tutti i file infettabili in base al loro formato. • esamina tutti i file infettabili in base alla loro estensione.
[/DISINFECT|/DELETE]	Azioni da eseguire su un oggetto infetto: • Disinfetta, elimina se la disinfezione non

/DISINFECT **/DELETE**	riesce. • Elimina. Commenti: • se non viene selezionata alcuna azione, l'oggetto sarà ignorato e le informazioni sul suo rilevamento verranno registrate nel report • i file compositi non saranno eliminati.
/W[A][!]:report_file **/W: report_file** **/WA: report_file**	Registrazione degli eventi nel report_file specificato: • solo eventi importanti; • tutti gli eventi. Il simbolo **!** viene utilizzato per forzare la sovrascrittura del file report ogni volta che viene avviata l'attività. È possibile utilizzare percorsi assoluti o relativi al file. Se il percorso contiene spazi, dev'essere digitato tra virgolette.

Esempio:

```
KAVSHELL SCAN "C:\Program Files" C:\Downloads\test.exe
/MEMORY /STARTUP /FA /DISINFECT /WA:log.txt
KAVSHELL SCAN /MEMORY /STARTUP C:\Downloads\test.exe /FC
/W:log.txt
```

9.2. Scansione completa

Sintassi del comando:

```
KAVSHELL FULLSCAN [/W[A][!]:report_file] [/D]
```

Se non vengono specificati i modificatori, verrà visualizzata la guida relativa alla sintassi del comando.

Le attività di scansione verranno eseguite con le impostazioni raccomandate dagli esperti di Kaspersky Lab.

/W[A][!]: report_file **/W: report_file** **/WA: report_file**	Registrazione degli eventi nel report_file specificato: • solo eventi importanti; • tutti gli eventi. Il simbolo **!** viene utilizzato per forzare la sovrascrittura del file report ogni volta che viene avviata l'attività. È possibile utilizzare percorsi assoluti o relativi al file. Se il percorso contiene spazi, dev'essere digitato tra virgolette.
/D	Annulla la scansione se questa attività è già stata eseguita con successo durante la giornata.

Esempi:

```
KAVSHELL FULLSCAN
KAVSHELL FULLSCAN /WA:fullscan.log
```

9.3. Avvio degli aggiornamenti

Sintassi del comando:

```
KAVSHELL UPDATE [updates_source] [/W[A][!]:report_file]
[/APP]
```

Se non vengono specificati i modificatori, verrà visualizzata la guida relativa alla sintassi del comando.

[**updates_source**]	Un server HTTP o FTP, oppure una cartella di rete dalla quale scaricare gli aggiornamenti. Se non viene specificato il percorso, le informazioni relative all'origine degli aggiornamenti verranno acquisite dall'attività di aggiornamento del database antivirus e dei moduli dell'applicazione.

/W[A][!]: report_file **/W: report_file** **/WA: report_file**	Registrazione degli eventi nel report_file specificato: • solo eventi importanti; • tutti gli eventi. Il simbolo **!** viene utilizzato per forzare la sovrascrittura del file report ogni volta che viene avviata l'attività. È possibile utilizzare percorsi assoluti o relativi al file. Se il percorso contiene spazi, dev'essere digitato tra virgolette.
/APP	Aggiornamento dei moduli dell'applicazione

Esempi:

```
KAVSHELL UPDATE ftp://ftp.kaspersky.com/
/WA:avbases_upd.txt
KAVSHELL UPDATE /APP
```

9.4. Ripristino della versione precedente del database antivirus

Sintassi del comando:

```
KAVSHELL ROLLBACK [/W[A][!]:report_file]
```

Se non vengono specificati i modificatori, verrà visualizzata la guida relativa alla sintassi del comando.

/W[A][!]: report_file **/W: report_file** **/WA: report_file**	Registrazione degli eventi nel report_file specificato: • solo eventi importanti; • tutti gli eventi. Il simbolo **!** viene utilizzato per forzare la sovrascrittura del file report ogni volta che viene avviata l'attività. È possibile utilizzare percorsi assoluti o relativi al file. Se il percorso contiene spazi, dev'essere digitato tra virgolette.

Esempi:

```
KAVSHELL ROLLBACK /WA:rollback.log
```

9.5. Modalità di protezione in tempo reale

Sintassi del comando:

KAVSHELL RTP [taskid] { /START [/PWD:password] | /STOP [/PWD:password] }

Se non vengono specificati i modificatori, verrà visualizzata la guida relativa alla sintassi del comando.

/START	Abilita la protezione in tempo reale o le relative attività specifiche.
/STOP	Disabilita la protezione in tempo reale o le relative attività specifiche.

taskid	Identificatore della protezione in tempo reale Se non viene specificato l'identificatore (dell'attività), alle attività di protezione in tempo reale saranno applicati tutti i comandi. I valori possibili sono: • on-access - protezione file in tempo reale; • mail-checker - protezione posta in tempo reale; • outlook-plugin - protezione posta di Microsoft Outlook in tempo reale; • script-checker - monitoraggio script in tempo reale; • office-guard - monitoraggio macro VBA
/PWD:password	Richiede la password dell'amministratore per eseguire il comando.

Esempi:

```
KAVSHELL RTP /START
KAVSHELL RTP on-access /START
KAVSHELL RTP /STOP script-checker /PWD:password
```

9.6. Avvio dell'applicazione

Sintassi del comando:

```
KAVSHELL START
```

9.7. Arresto dell'applicazione

Sintassi del comando:

```
KAVSHELL STOP [/PWD:password]
```

/PWD:password	Immissione della password dell'amministratore richiesta per eseguire il comando.

Esempio:

```
KAVSHELL STOP
```

9.8. Gestione delle attività

Sintassi del comando:

```
KAVSHELL TASK [ taskid {/START [/W[A][!]:report_file]|
      /STOP |
      /PAUSE |
      /RESUME [/W[A][!][: report_file]]|
      /DELETE } ] [/PWD:password]
```

Se non vengono specificati modificatori, verrà visualizzata la guida per la sintassi, unitamente agli identificatori univoci e allo stato di ciascuna attività.

/START	Avvia l'attività con l'identificatore specificato.
/W[A][!]:report_file **/W:report_file** **/WA:report_file**	Registrazione degli eventi nel report_file specificato: • solo eventi importanti; • tutti gli eventi. Il simbolo **!** viene utilizzato per forzare la sovrascrittura del file report ogni volta che viene avviata l'attività. È possibile utilizzare percorsi assoluti o relativi al file. Se il percorso contiene spazi, dev'essere digitato tra virgolette.
/STOP	Arresta l'attività con l'identificatore specificato. La password è un parametro obbligatorio richiesto per arrestare le attività di protezione in tempo reale! Tali attività comprendono: • la protezione file in tempo reale; • la protezione posta in tempo reale; • il monitoraggio script in tempo reale; • il monitoraggio delle macro VBA; • la protezione contro gli attacchi di rete.
/PAUSE	Sospende l'attività con l'identificatore specificato.

/RESUME	Riprende l'attività con l'identificatore fornito.
/DELETE	Elimina l'attività con l'identificatore fornito.
taskid	Identificatori univoci delle attività. È possibile gestire le attività di sistema tramite i seguenti identificatori standard: • scan-computer - scansione completa del computer; • scan-removable - scansione delle unità removibili; • scan-quarantine - scansione della quarantena; • scan-critical - scansione dei settori di boot del disco, della memoria e degli oggetti di avvio; • update-bases - aggiornamento del database antivirus; • update-app - aggiornamento dei moduli dell'applicazione; • rollback - ripristino della versione precedente del database antivirus; • on-access - protezione file in tempo reale; • mail-checker - protezione posta in tempo reale; • script-checker - monitoraggio script in tempo reale; • office-guard - monitoraggio delle macro VBA; • ids - protezione contro gli attacchi di rete.
/PWD:password	Immissione della password dell'amministratore richiesta per eseguire un comando

Esempi:

```
KAVSHELL TASK
```

```
KAVSHELL TASK update-app /START /WA:fullscan.log
KAVSHELL TASK _LOCAL_0630cddf-0793-4c2d-be1e-a3daed0904c6
/DELETE
```

9.9. Importazione/esportazione delle impostazioni

Sintassi del comando:

KAVSHELL IMPORT settings_file [/PWD:password]

KAVSHELL EXPORT settings_file [/PWD:password]

settings_file	Il nome del file profilo da cui verranno importate le impostazione di Kaspersky Anti-Virus (o nel quale verranno esportate). Per dettagli sui profili, vedere la sezione 5.10.3 a pagina 113).
/PWD:password	Immissione della password dell'amministratore richiesta per eseguire il comando.

Esempi:

```
KAVSHELL IMPORT c:\kav50settings.xml
KAVSHELL EXPORT c:\kav50settings.xml
```

9.10. Aggiunta di una chiave di licenza

Sintassi del comando:

KAVSHELL ADDKEY file [/R] [/PWD:password]

file	Nome del file della chiave di licenza.
[/R]	Sostituzione della chiave di licenza corrente con una nuova chiave.
/PWD:password	Immissione della password dell'amministratore richiesta per eseguire il comando.

Esempio:

```
KAVSHELL ADDKEY c:\00A531D2.key /R
```

CAPITOLO 10. DOMANDE FREQUENTI

Questo capitolo è dedicato alle domande più frequenti poste dai nostri utenti sull'installazione, la configurazione e il funzionamento di Kaspersky Anti-Virus; faremo il possibile per fornire risposte più esaurienti possibile.

Domanda: È possibile usare Kaspersky Anti-Virus con programmi antivirus di altri produttori?

Per evitare conflitti di software, si consiglia di disinstallare eventuali altri programmi antivirus presenti nel computer prima di installare Kaspersky Anti-Virus.

Domanda: Kaspersky Anti-Virus non riesamina i file già esaminati in precedenza. Perché?

È vero. Kaspersky Anti-Virus non riesamina i file che non sono stati modificati dalla scansione precedente.

Questo è possibile grazie alle nuove tecnologie iChecker e iStreams. La tecnologia è implementata nel programma utilizzando un database di checksum dei file e un metodo di archiviazione delle stesse nei flussi NTFS supplementari.

Domanda: Perché Kaspersky Anti-Virus rallenta le prestazioni del server e impone un carico notevole sulla CPU?

La ricerca dei virus è un problema matematico che comporta un'intensa attività di elaborazione e richiede l'analisi strutturale, il calcolo delle "checksum" e la conversione dei dati matematici. Per questo motivo la velocità del processore è la principale risorsa consumata da Kaspersky Anti-Virus, e ogni nuovo virus aggiunto al database antivirus aumenta la durata complessiva della scansione. Si tratta di un compromesso necessario per la sicurezza dei dati custoditi nel computer.

A differenza di altri produttori di software antivirus che accelerano il processo di scansione escludendo dai propri database i virus più difficilmente rilevabili o meno frequenti nella regione geografica del rivenditore del prodotto ed i formati di file che richiedono complesse analisi (per esempio i file PDF),

Kaspersky Lab ritiene che la funzione di Kaspersky Anti-Virus consista nel garantire ai propri utenti una sicurezza completa ed efficace. Riteniamo che una "protezione parziale" sia perfino peggiore di una protezione del tutto assente, che almeno obbliga l'utente ad adottare delle precauzioni.

Kaspersky Anti-Virus offre ai propri utenti il massimo della protezione. Gli utenti più esperti hanno ovviamente la possibilità di accelerare il processo di scansione antivirus a discapito della sicurezza globale disattivando l'analisi di determinati tipi di file, ma questo tipo di operazione è sconsigliato a chi desidera la massima sicurezza.

Per garantire all'utente la massima protezione, Kaspersky Anti-Virus riconosce oltre 1200 formati di archivi e file compressi, ed è in grado di disinfettarne 6. Ciò è essenziale per la protezione antivirus, poiché i codici eseguibili dannosi possono annidarsi all'interno di file di qualsiasi formato riconosciuto. Tuttavia, a dispetto dell'incremento quotidiano del numero di virus rilevati da Kaspersky Anti-Virus e del numero sempre crescente di formati di file riconosciuti, ogni nuova versione del prodotto funziona più velocemente delle precedenti. Ciò è possibile grazie all'uso di nuove tecnologie esclusive come iChecker™ e i-Streams™, sviluppate da Kaspersky Lab.

Domanda: Perché mi occorre un file chiave di licenza? La mia copia di Kaspersky Anti-Virus può funzionare senza?

No, senza chiave di licenza Kaspersky Anti-Virus non funziona.

Se non si è ancora deciso di acquistare Kaspersky Anti-Virus, è possibile acquistare una versione di prova dell'applicazione dal sito Web di Kaspersky Lab, sezione **Downloads → Trial Version**. Tale versione di prova funzionerà per 15 giorni, al termine dei quali la chiave viene bloccata.

Domanda: Cosa succede alla scadenza della licenza?

Alla scadenza della licenza, Kaspersky Anti-Virus continuerà a funzionare, ma non sarà possibile aggiornare il database antivirus. Kaspersky Anti-Virus continuerà a disinfettare gli oggetti infetti, utilizzando però un database obsoleto.

In questo caso, si consiglia di informare il proprio amministratore di sistema e di rivolgersi al rivenditore presso cui è stato acquistato Kaspersky Anti-Virus o direttamente a Kaspersky Lab per rinnovare la licenza.

Domanda: Perché eseguire gli aggiornamenti quotidianamente?

Qualche anno fa i virus venivano trasmessi tramite i dischi floppy, ed era possibile garantire una protezione adeguata del computer installando un programma antivirus il cui database veniva aggiornato di quando in quando. Le più recenti epidemie informatiche si diffondono invece in tutto il mondo nel giro di poche ore, e Kaspersky Anti-Virus con un database obsoleto potrebbe essere inerme contro le nuove minacce. Per evitare rischi per il proprio computer, è quindi opportuno aggiornare il database antivirus quotidianamente.

Di anno in anno, Kaspersky Lab intensifica la frequenza degli aggiornamenti del database antivirus. Attualmente la frequenza di aggiornamento è oraria.

L'aggiornamento dei moduli dell'applicazione di Kaspersky Anti-Virus è una funzione supplementare che consente sia la correzione delle vulnerabilità identificate e l'aggiunta di nuove funzioni.

Domanda: Quali modifiche sono state apportate al servizio di aggiornamento della versione 5.0?

La serie 5.0 della suite di prodotti Kaspersky Lab prevede un nuovo servizio di aggiornamento sviluppato secondo le richieste dei nostri utenti. La procedura di aggiornamento è ora completamente automatizzata, dalla preparazione degli aggiornamenti in Kaspersky Lab al momento in cui i file vengono aggiornati sui computer dei clienti.

I vantaggi del nuovo servizio di aggiornamento comprendono:

- *La capacità di riprendere il download dei file dal punto in cui si era interrotto in seguito a una disconnessione*. Al ripristino della connessione, vengono prelevati solo i file non scaricati in precedenza.
- *Le dimensioni degli aggiornamenti cumulativi sono dimezzate*. Gli aggiornamenti cumulativi contengono l'intero database antivirus e sono di dimensioni notevolmente maggiori rispetto ai comuni aggiornamenti. Il nuovo servizio applica una speciale tecnologia che consente di utilizzare il database antivirus esistente per il processo di aggiornamento cumulativo.
- *Download accelerato da Internet*. Kaspersky Anti-Virus seleziona un server di aggiornamento Kaspersky Lab ubicato nella regione dell'utente. Inoltre, i server vengono assegnati in base a quanto sono impegnati. In tal modo, l'utente non viene assegnato ad un

server sovraccarico ma verso uno che risulta disponibile in quel momento.

- *Uso di "liste nere" di chiavi di licenza*. Gli utenti illegali e privi di licenza non possono più accedere al servizio di aggiornamento. In tal modo gli utenti che invece sono in possesso di regolare licenza non subiranno ritardi dovuti al sovraccarico dei server di aggiornamento.
- Le aziende sono oggi in grado di creare un server locale di aggiornamento. Questa funzione è progettata per le aziende in cui i computer protetti tramite i prodotti Kaspersky Lab sono uniti da una singola LAN. Qualsiasi computer della LAN può essere trasformato in server di aggiornamento che scarica gli aggiornamenti da Internet e li condivide con gli altri computer in rete.

Domanda: È possibile che un pirata informatico sostituisca il mio database antivirus?

Ogni database antivirus è dotato di firma esclusiva verificata da Kaspersky Anti-Virus al momento dell'accesso al database. Se la firma non è corretta o la data del database è successiva a quella di scadenza della licenza, Kaspersky Anti-Virus non lo utilizzerà.

Domanda: Come posso configurare l'aggiornamento da Internet per un singolo computer in modo da consentire la condivisione dei file scaricati con gli altri computer della rete?

Supponiamo che il computer da aggiornare tramite Internet sia il "server" e tutti gli altri computer siano i "client" di quel server.

Esistono diversi metodi per configurare l'aggiornamento in una LAN:

- Abilitare l'uso di un'origine locale degli aggiornamenti in un server di Kaspersky Administration Kit 5.0.
  Kaspersky Administration Kit offre una funzionalità integrata per la distribuzione degli aggiornamenti all'interno di reti aziendali. Può aggiornare un'origine degli aggiornamenti condivisa secondo una frequenza programmata e avviare le attività di aggiornamento sugli altri computer. Kaspersky Administration Kit controlla quindi che il volume dei dati scaricati da Internet non superi le necessità effettive delle applicazioni installate. È possibile consultare l'elenco delle patch disponibili sul server: Per informazioni dettagliate sulla configurazione, consultare la guida dell'amministratore di Kaspersky Administration Kit 5.0.
- Abilitare l'uso di un'origine locale degli aggiornamenti in uno dei prodotti di Kaspersky Lab

Utilizzare questa opzione quando è impossibile utilizzare Kaspersky Administration Kit, o quando è necessario organizzare una struttura più complicata di reti di server degli aggiornamenti. Per fare ciò:

- Individuare i computer da adibire a server degli aggiornamenti. Su di essi devono essere installate le applicazioni Kaspersky Lab (versione 5.0).
- Creare una risorsa di rete da usare per l'ulteriore condivisione degli aggiornamenti su ciascuno dei computer selezionati. Può trattarsi di una cartella di rete su un computer Windows, oppure di un server FTP o HTTP. Definire i diritti di accesso corretti per quella cartella.
- Creare una nuova attività di aggiornamento o modificarne una esistente. Abilitare la condivisione degli aggiornamenti attraverso un'origine locale e specificare la cartella creata.
- Specificare la cartella locale degli aggiornamenti del server come origine degli aggiornamenti su tutti i computer che devono essere aggiornati da quel server.

Domanda:Uso un server proxy e l'aggiornamento non funziona sul mio computer. Cosa posso fare?

L'incapacità di prelevare gli aggiornamenti se si utilizza un server proxy può essere provocata dai seguenti problemi:

- Impostazioni di rete errate.

  Esistono due opzioni per la configurazione delle impostazioni di rete durante la configurazione del servizio di aggiornamento: si possono utilizzare le impostazioni di MS Internet Explorer o impostazioni personalizzate. Il servizio di aggiornamento a volte utilizza erroneamente le impostazioni di MS Internet Explorer. Ciò può verificarsi nei seguenti casi:

La connessione Internet non è configurata sul computer;

le impostazioni di MS Internet Explorer non sono disponibili se nessuno degli utenti è collegato;

il server proxy richiede l'autorizzazione.

  In tutti questi casi, è necessario specificare i parametri di rete direttamente nelle impostazioni del servizio di aggiornamento.

- Il server proxy utilizzato appartiene a un tipo non supportato dal servizio di aggiornamento di Kaspersky Anti-Virus.

Il servizio di aggiornamento non funziona attraverso Kerio WinRoute, poiché WinRoute non supporta pienamente il protocollo HTTP 1.0. In questo caso si consiglia di utilizzare un qualsiasi altro server proxy.

Il servizio di aggiornamento non funziona neanche attraverso Microsoft ISA Server con protocollo FTP. In questo caso si consiglia di procurarsi gli aggiornamenti dai server di Kaspersky Lab tramite il protocollo HTTP.

Domanda: Dopo l'installazione di Kaspersky Anti-Virus, la mia connessione alla rete locale/a Internet non funziona. Cosa posso fare?

Ciò significa che esiste un conflitto tra il modulo di protezione contro gli attacchi di rete di Kaspersky Lab e il firewall installato sul computer.

Per ripristinare la connessione alla rete locale/a Internet, sarà necessario disabilitare la protezione contro gli attacchi di rete. Per fare ciò:

1. Aprire la finestra principale dell'applicazione di Kaspersky Anti-Virus e passare alla scheda **Impostazioni** (vedere la Figura 3).
2. Utilizzando il collegamento Configura protezione in tempo reale, aprire la finestra di dialogo **Impostazione della protezione in tempo reale** e passare alla scheda **Rete** (vedere la Figura 24).
3. Deselezionare la casella **Abilita la protezione in tempo reale contro gli attacchi di rete** e scegliere il pulsante **OK**.

Per applicare le impostazioni appena configurate è necessario riavviare il computer. Per fare ciò, scegliere il pulsante **Sì**. Se si desidera riavviare il computer successivamente, scegliere il pulsante **No**.

Domanda: Dopo avere installato Kaspersky Anti-Virus, il mio sistema operativo ha iniziato a comportarsi in maniera strana (schermate blu, riavvio ripetuto del computer, ecc.). Cosa posso fare?

Ciò significa che esiste un conflitto di funzionamento tra Kaspersky Anti-Virus e qualche altro software installato sul computer. Per ripristinare il funzionamento del sistema operativo:

1. Non appena il computer inizia la procedura di boot, premere il tasto **F8** finché non vengono visualizzate le opzioni di avvio del sistema operativo:
2. Selezionare la voce **Modalità provvisoria** e avviare il sistema operativo.

3. Avviare Kaspersky Anti-Virus.
4. Nella finestra principale dell'applicazione, passare alla scheda **Impostazioni** e scegliere il collegamento Impostazioni supplementari.
5. Nella finestra di dialogo **Impostazioni supplementari** che verrà visualizzata, passare alla scheda **Sicurezza** (vedere la Figura 61) e deselezionare la casella **Esegui Kaspersky Anti-Virus all'avvio del sistema**. Scegliere il pulsante **OK**.
6. Riavviare il sistema operativo normalmente.

A questo punto, contattare il Servizio di assistenza tecnica visitando il sito Web di Kaspersky Lab (sezione **Services → Technical Support → Send a question to the support service**). Descrivere il problema e le condizioni nelle quali si verifica il più dettagliatamente possibile.

Non si dimentichi di allegare quanto segue alla domanda:

- file memory dump completo (informazioni dettagliate sulla creazione di tale file sono disponibili sul sito Web di Kaspersky Lab, sezione **Services→ Tecnical Support → Troubleshooting → Obtaining a full memory dump file in case of a system failure**);
- Il file report dell'utility **GetSystemInfo** (questa utility e le istruzioni dettagliate su come ottenere un report è disponibile per il download sul sito Web di Kaspersky Lab, sezione **Services → Technical support → Troubleshooting → Obtaining a GetSystemInfo report**);

APPENDICE A. CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA

Kaspersky Anti-Virus offre assistenza tramite il Servizio di assistenza tecnica di Kaspersky Lab nei seguenti casi:

- Si ritiene che l'applicazione funzioni in maniera anomala e irregolare.
- Kaspersky Anti-Virus ha rilevato un file sospetto contenente informazioni importanti e lo ha bloccato. Si desidera però continuare a utilizzare tale file.

Per inviare un messaggio al Servizio di assistenza tecnica relativo a qualsiasi problema di funzionamento del programma,

usare il collegamento Invia domanda ad assistenza tecnica nella sezione sinistra della scheda **Assistenza** (vedere la 4) nella finestra principale del programma.

Facendo clic sul collegamento si apre automaticamente la finestra del client di posta elettronica installato sul computer, ad esempio MS Outlook, e si crea un messaggio di posta elettronica contenente un file di testo con la descrizione del sistema e tutti i dati necessari relativi a Kaspersky Anti-Virus. Descrivere in maniera dettagliata il problema riscontrato durante l'uso di Kaspersky Anti-Virus e inviare il messaggio. Il Servizio di assistenza tecnica si metterà in contatto con l'utente al più presto.

È possibile modificare l'indirizzo di posta elettronica che verrà utilizzato per inviare le domande al Servizio di assistenza tecnica nella scheda **Generale** (vedere la Figura 58) della finestra delle impostazioni supplementari di Kaspersky Anti-Virus (ad esempio, è possibile inserire l'indirizzo dell'amministratore della sicurezza), oppure specificare l'URL da aprire quando si richiede assistenza tecnica.

Se Kaspersky Anti-Virus ha messo in quarantena un file sospetto, è possibile aggiornare il database antivirus e cercare di disinfettarlo (vedere la sezione 5.10.1.2 a pagina 105). Tuttavia, se è impossibile disinfettare l'oggetto ma si desidera recuperarlo al più presto, è possibile inviarlo a Kaspersky Lab per farlo esaminare. Il file potrebbe essere stato infettato da un virus sconosciuto, o potrebbe trattarsi più semplicemente di un falso allarme.

Attenzione! È possibile inviare i file sospetti a Kaspersky Lab solo se sono stati esaminati con il database antivirus aggiornato nel giorno in cui si sta inviando tale file.

Per inviare un file sospetto a Kaspersky Lab per un'analisi approfondita,

selezionare il file sospetto nella finestra **Quarantena** (vedere la sezione 5.10.1.2 a pagina 105) e scegliere il pulsante Invia.

Il pulsante apre automaticamente la finestra del client di posta elettronica installato sul computer, per esempio MS Outlook Express, e crea un messaggio di posta elettronica con allegato il file sospetto. Inviare il messaggio. Gli esperti di Kaspersky Lab analizzeranno con attenzione il file ricevuto, cercando di recuperare tutti i dati in esso contenuti. Infine invieranno all'utente un report completo con i risultato dell'analisi del file.

Si noti che non è possibile inviare a Kaspersky Lab più di tre file da analizzare in un giorno. Ogni file deve essere stato esaminato con Kaspersky Anti-Virus il cui database è stato aggiornato al massimo tre giorni prima dell'invio.

In alcuni casi ci possono essere valide ragioni per considerare infetti dei file anche se Kaspersky Anti-Virus non ha rilevato la presenza di virus durante la scansione. Anche tali file possono essere inviati a Kaspersky Lab per un'analisi.

Per inviare a Kaspersky Lab i file in cui si sospetta la presenza di virus per farli analizzare,

usare il collegamento Invia file per analisi nella parte sinistra della scheda **Assistenza** (vedere la figura 4). Selezionare i file sospetti tramite la finestra di ricerca standard.

La procedura di invio di un messaggio di posta elettronica a Kaspersky Lab è del tutto identica a quella descritta per inviare oggetti sospetti messi in quarantena.

APPENDICE B. GLOSSARIO

Questi documenti si basano su concetti e terminologia specifici del settore della protezione antivirus. Questo glossario può essere consultato come un dizionario contenente le definizioni di tali concetti. Per praticità è organizzato in ordine alfabetico.

A

Administration agent - speciale applicazione che provvede all'interazione tra un server di amministrazione e le applicazioni dei prodotti Kaspersky Lab per le aziende. È inclusa in Kaspersky Administration Kit 5.0.

Consolle di amministrazione - componente che fornisce l'interfaccia grafica per la gestione di Kaspersky Anti-Virus. È inclusa in Kaspersky Administration Kit 5.0.

Gruppo di amministrazione - un insieme di computer riuniti in un unico gruppo per comodità di controllo. Il gruppo è gestito come una singola unità e può disporre di una regola di gruppo, contenere sottogruppi e ricevere comandi amministrativi.

Server di amministrazione - speciale applicazione avente funzioni di controllo e di archiviazione centralizzata dei dati per le applicazioni Kaspersky Lab installate in una rete aziendale. È inclusa in Kaspersky Administration Kit 5.0.

AdWare - codice software per dimostrazioni pubblicitarie aggiunto ai programmi senza informarne l'utente. Di norma, l'adware viene integrato nei software gratuiti. L'annuncio pubblicitario appare nell'interfaccia del programma. Spesso tali programmi raccolgono e trasmettono ai propri sviluppatori delle informazioni personali sugli utenti, modificano vari parametri dei browser (home page e pagine di ricerca, livelli di sicurezza, ecc.), generando ulteriore traffico non controllabile dagli utenti. Tutto ciò può provocare violazioni delle regole di sicurezza o addirittura causare perdite finanziarie.

Flussi NTFS supplementari (flussi NTFS) - flussi di dati in un'unità con file system NTFS che integrano il flusso principale che ne contiene i contenuti.

Database antivirus - database creato dagli specialisti di Kaspersky Lab, contenente descrizioni dettagliate di tutti i virus esistenti al momento della compilazione e dei metodi per la loro individuazione ed eliminazione. Il nostro database viene aggiornato continuamente con informazioni su nuovi virus, pertanto è necessario mantenerlo aggiornato per garantire la protezione costante del computer.

Stato della protezione antivirus - stato attuale della protezione antivirus, che caratterizza il livello di sicurezza del computer.

Plug-in di gestione dell'applicazione - componente specializzato che fornisce un'interfaccia per il controllo remoto dell'applicazione tramite una console di amministrazione. Ogni applicazione richiede il proprio plug-in di gestione, che pertanto è compreso nel pacchetto di qualsiasi applicazione Kaspersky Lab che possa essere controllata tramite Kaspersky Administration Kit 5.0.

Moduli dell'applicazione - file presenti nel kit di distribuzione di Kaspersky Anti-Virus 5.0 for Windows Workstations, che garantiscono l'implementazione delle principali attività dell'applicazione. Per ogni tipo di attività implementata da Kaspersky Anti-Virus (*protezione in tempo reale*, *scansione manuale*, *aggiornamenti*) esiste un corrispondente modulo eseguibile. Avviando la scansione completa del computer dalla finestra principale dell'applicazione, si esegue il modulo corrispondente a questa attività.

Aggiornamenti disponibili - Service Pack contenenti una raccolta di aggiornamenti e modifiche strutturali urgenti, accumulatisi in uno specifico arco di tempo.

B

Backup - creazione e archiviazione di una copia di un file prima del trattamento (riparazione o cancellazione). Tale file potrà successivamente essere ripristinato dalla copia di backup, qualora si desideri, ad esempio, eseguirne la scansione con una versione aggiornata dell'antivirus.

Memoria di backup - area riservata all'archiviazione delle copie di backup degli oggetti create prima di disinfettarli o eliminarli.

"Lista nera" - database contenente informazioni sulle chiavi di licenza appartenenti a individui che hanno violato il contratto di licenza, e sulle chiavi che sono state generate ma che per qualsiasi motivo sono rimaste invendute. Il contenuto della lista nera viene aggiornato insieme al database antivirus, e Kaspersky Anti-Virus non funziona senza di essa.

C

Controllo centralizzato dell'applicazione - controllo dell'applicazione tramite i servizi di amministrazione messi a disposizione da Kaspersky Administration Kit 5.0.

Chiave di licenza corrente - chiave di licenza installata ed attualmente utilizzata da Kaspersky Anti-Virus per sbloccare le proprie funzioni. Essa determina il periodo di validità della licenza e le regole della stessa riguardo all'utilizzo del prodotto. Una applicazione non può avere più di una chiave "corrente".

D

Eliminazione di un oggetto - metodo di trattamento di un oggetto. Eliminare un oggetto significa rimuoverlo fisicamente dal computer. È il

metodo raccomandato per il trattamento degli oggetti infetti. Se l'eliminazione è la prima azione da eseguire su un oggetto, è necessario crearne una copia di backup prima di procedere. Il backup consente l'eventuale ripristino dell'oggetto eliminato.

Disinfezione - uno dei metodi di trattamento degli *oggetti infetti*. La disinfezione può permettere il recupero parziale o totale dei dati, o portare alla conclusione che il file non può essere riparato. Gli oggetti vengono riparati tramite il database antivirus. Se la riparazione è la prima azione da eseguire, ad esempio dopo l'individuazione di un oggetto sospetto, l'applicazione crea una copia di backup del file in questione. Se alcuni dati vanno perduti durante la disinfezione, il backup può essere utilizzato per il loro recupero.

Disinfezione di oggetti al riavvio - metodo per il trattamento degli oggetti infetti che, al momento della riparazione, sono utilizzati da altre applicazioni. Questo metodo crea una copia dell'oggetto infetto, la ripara e la sostituisce all'originale infetto al successivo riavvio del computer. Nei sistemi operativi MS Windows 9x, la disinfezione di file con un nome lungo al riavvio ne determina la sostituzione forzata con copie disinfettate dal nome più breve. Ciò può provocare anomalie di funzionamento delle applicazioni che utilizzano oggetti disinfettati in tal modo.

E

Database di posta - database contenente i messaggi di posta elettronica salvati nel computer. Ogni messaggio in arrivo o in uscita viene salvato nel database subito dopo la ricezione o l'invio. La scansione del database viene eseguita in modalità manuale.

Esclusioni - impostazioni definite dall'utente, che escludono dalla scansione certi oggetti. Le regole di esclusione dalla protezione in tempo reale e dalla scansione manuale possono essere personalizzate. Si possono ad esempio escludere gli archivi da una scansione completa, o utilizzare maschere per escludere dei file.

Database antivirus esteso - *database standard* al quale viene aggiunto un database supplementare che agevola l'intercettazione di software potenzialmente pericolosi sul computer dell'utente.

F

Maschera di file - è una rappresentazione del nome e dell'estensione di un file con simboli generici. I due simboli principali utilizzati nelle maschere dei file sono "*" e "?" (in cui "*" sostituisce un numero qualsiasi di caratteri e "?" ne sostituisce uno solo). Tramite questi simboli è possibile rappresentare qualsiasi file. Si noti che il nome e l'estensione di un file sono sempre separati da un punto.

Scansione completa - modalità di funzionamento dell'applicazione che prevede una scansione completa del computer su richiesta dell'utente

alla ricerca di codici ostili, seguita dalla disinfezione o eliminazione degli oggetti infetti o sospetti eventualmente rilevati.

G

Regola di gruppo - insieme di parametri che regolano la funzionalità dell'applicazione in un gruppo di amministrazione controllato tramite Kaspersky Administration Kit 5.0.

H

Hack Tool - software utilizzati dai pirati informatici per accedere ai computer altrui. Questa categoria comprende vari tipi di scanner illegali di vulnerabilità, strumenti per la violazione delle password ed altri tipi di software per penetrare nelle risorse di rete o violare un sistema per attaccarlo.

Alta velocità - livello di protezione del computer che garantisce le massime prestazioni del sistema riducendo il numero di oggetti esaminati.

I

iChecker™ - tecnologia che consente all'applicazione di escludere da una scansione tutti gli oggetti che non hanno subito modifiche dalla scansione precedente. Questa tecnologia è implementata tramite un database di checksum degli oggetti.

Oggetto infetto - oggetto contenente un codice dannoso. Si consiglia di interrompere qualsiasi attività con questi oggetti poiché possono infettare il computer.

iStreams™ - tecnologia che consente all'applicazione di escludere da una scansione gli oggetti ubicati su unità con file system NTFS che non hanno subito modifiche dalla scansione precedente. Questa tecnologia è implementata sulla base dell'archiviazione di checksum in flussi NTFS supplementari.

J

Joke - software che non infligge direttamente alcun danno al computer, ma che visualizza messaggi che comunicano ingannevolmente che sono stati inflitti o saranno inflitti danni in certe condizioni. Questi programmi spesso mettono in guardia l'utente da un pericolo che non esiste, ad esempio visualizzano messaggi relativi alla formattazione del disco (nonostante la formattazione non sia in esecuzione), "rilevano" virus in file non infetti, ecc.

K

Kaspersky Administration Kit 5.0 - applicazione compresa in Kaspersky Business Optimal e Kaspersky Corporate Suite, concepita per l'amministrazione centralizzata di un sistema di protezione antivirus in una rete aziendale, basata sulle applicazioni Kaspersky Lab.

L

Chiave di licenza - file con estensione *key* che funge da "chiave" personale. Questo file è necessario per il funzionamento corretto di Kaspersky Anti-Virus. Tale file è incluso nel kit di distribuzione, se Kaspersky Anti-Virus è stato acquistato presso un rivenditore Kaspersky Lab. Se il prodotto è stato acquistato online, la chiave di licenza viene spedita all'acquirente per posta elettronica. Senza la chiave di licenza, Kaspersky Anti-Virus NON FUNZIONA.

Periodo di validità - periodo durante il quale l'utente ha diritto di avvalersi della piena funzionalità di Kaspersky Anti-Virus. Di norma, tale periodo definito dalla chiave di licenza ha la durata di un anno solare a partire dal momento di attivazione della chiave. Una volta scaduta la licenza, il prodotto continuerà ad operare, ma non sarà più possibile eseguire gli aggiornamenti del *database antivirus* e dei *moduli dell'applicazione*.

Amministratore della rete logica - addetto al controllo del funzionamento dell'applicazione tramite il sistema di amministrazione remota centralizzata Kaspersky Administration Kit.

M

Protezione massima - livello di protezione del computer corrispondente alla massima protezione possibile, che comporta una certa riduzione delle prestazioni.

O

Blocco dell'oggetto - negazione dell'accesso a un oggetto da parte di applicazioni esterne. Un oggetto bloccato non può essere letto, eseguito, modificato o rimosso.

Oggetto OLE - oggetti o documenti incorporati in altri file mediante la tecnologia OLE.

Q

Quarantena - speciale forma di archiviazione dei dati, ideata per isolare gli oggetti sospetti.

Messa in quarantena - metodo di gestione degli *oggetti sospetti* che blocca l'accesso a tali oggetti e li trasferisce nella cartella della quarantena per successivo trattamento.

R

Protezione in tempo reale - modalità di funzionamento in cui l'applicazione risiede permanentemente nella memoria del computer, monitorando tutte le chiamate agli oggetti del file system. Prima di concedere l'accesso ad un oggetto, l'applicazione lo esamina e, se viene individuato un virus, disinfetta o elimina l'oggetto, oppure blocca l'accesso ad esso (a seconda delle impostazioni definite dall'utente).

Livello raccomandato - livello di protezione antivirus predefinito secondo le impostazioni raccomandate dagli esperti di Kaspersky Lab, che assicura il miglior compromesso tra protezione e prestazioni.

Recupero, ripristino - spostamento di un file dalla cartella di *quarantena* o *backup* a una cartella di destinazione specificata o a quella originaria in cui si trovava prima della quarantena, della disinfezione o dell'eliminazione.

Chiave di licenza di riserva - chiave di licenza installata per permettere il corretto funzionamento di Kaspersky Anti-Virus, ma non ancora attivata. Tale chiave viene attivata allo scadere della licenza corrente.

Riskware - programmi che non sono virus ma che costituiscono comunque una potenziale minaccia. In certe condizioni, la presenza di tali programmi sul computer può costituire una minaccia per i dati. Tali programmi comprendono i software di amministrazione remota, i dialer automatici che connettono a siti Internet a pagamento tramite la connessione dial-up, ecc.

Rootkit - utility che consentono di celare le azioni nocive. Esse "nascondono" il malware in modo che non possa essere rilevato dai programmi anti-virus. I rootkit possono inoltre modificare il sistema operativo, alterandone le funzioni principali per nascondere la loro presenza e le azioni eseguite dal pirata informatico sul computer infetto.

S

Esamina oggetti infettabili, per estensione - durante la scansione, l'applicazione prende in considerazione le estensioni dei file.

Esamina oggetti infettabili, per formato - durante la scansione, l'applicazione analizza il contenuto dei file, ovvero l'identificatore del formato nell'intestazione del file.

Amministratore della sicurezza -addetto al controllo del funzionamento dell'applicazione. L'amministratore può agire a distanza tramite la *Consolle di amministrazione* o utilizzare l'interfaccia locale.

File di impostazioni - file contenente le impostazioni generali del programma. Le impostazioni del software possono essere esportate (salvate) in un file di questo tipo o importate (caricate) dal file in cui sono state salvate.

SpyWare - software progettato per accedere senza autorizzazione ai dati dell'utente, ricostruire la cronologia delle azioni eseguite su un computer e raccogliere informazioni sul contenuto dei dischi rigidi. Questi strumenti consentono ai pirati informatici di ottenere dati o perfino di controllare un computer dall'esterno. Gli spyware sono generalmente distribuiti con i software gratuiti e si installano su un computer senza che l'utente se ne renda conto. Questa categoria comprende software in grado di ricostruire le sequenze di tasti premuti sulla tastiera, strumenti per la violazione delle password, programmi per la raccolta di dati confidenziali (per esempio, i numeri di carte di credito).

Database antivirus standard - database antivirus che consente di rilevare tutti i programmi dannosi esistenti e di disinfettare gli oggetti e i dati colpiti.

Oggetti d'avvio - insieme di programmi necessari per l'esecuzione e il corretto funzionamento del sistema operativo e di altri programmi installati nel computer. Il sistema operativo li esegue ad ogni avvio. Alcuni virus cercano di infettarli e possono provocare un errore di avvio.

Oggetto sospetto - oggetto contenente una modifica del codice di un virus noto o un codice somigliante a quello di un virus ma ancora sconosciuto a Kaspersky Lab.

T

Attività - azione specifica eseguita da un'applicazione di Kaspersky Lab.

Processi attendibili - elenco dei processi software le cui attività con i file non vengono monitorate in tempo reale da Kaspersky Anti-Virus. Ciò significa che tutti gli oggetti avviati, aperti o salvati da un processo attendibile non vengono esaminati.

U

Virus ignoto - nuovo virus non ancora registrato nel *database antivirus*. Di regola, Kaspersky Anti-Virus rileva i virus ignoti per mezzo dell'*analizzatore euristico di codici* e indica come *sospetti* gli oggetti che li contengono.

Aggiornamento - procedura di sostituzione/aggiunta di nuovi file (database antivirus o moduli dell'applicazione) scaricati dai server di aggiornamento di Kaspersky Lab.

Server di aggiornamento di Kaspersky Lab - elenco di server http e ftp appartenenti a Kaspersky Lab, da cui Kaspersky Anti-Virus copia nel computer il database antivirus e i moduli dell'applicazione aggiornati.

Aggiornamenti urgenti - aggiornamenti critici dei moduli dell'applicazione.

V

Unità virtuali (RAM drive) - area della RAM in un computer che emula un normale disco fisico.

APPENDICE C. KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab è ormai un leader indiscusso nel settore delle tecnologie per la sicurezza informatica. Produce una vasta gamma di applicazioni per la sicurezza dei dati e offre soluzioni complete di alto livello per garantire la sicurezza di computer e reti contro ogni tipo di programma dannoso, messaggi di posta elettronica non richiesti e indesiderati e attacchi di pirateria informatica.

Kaspersky Lab è un azienda internazionale, con sede nella Federazione Russa e uffici di rappresentanza nel Regno Unito ed in Francia, Germania, Giappone, USA (CA), Benelux, Cina, Polonia e Romania. Recentemente è stato inaugurato un nuovo reparto, l'European Anti-Virus Research Centre, in Francia. Kaspersky Lab conta su una rete di partner costituita da oltre 500 aziende in tutto il mondo.

Oggi Kaspersky Lab si avvale di oltre 450 esperti, tutti specializzati in tecnologie antivirus, 10 dei quali in possesso di laurea in amministrazione aziendale, 16 di specializzazione postlaurea, e due appartenenti alla Computer Anti-Virus Researcher's Organization (CARO).

Kaspersky Lab offre soluzioni di sicurezza di alto livello, elaborate grazie a un'esperienza esclusiva accumulata in più di 14 anni di attività nel settore dei virus informatici. La scrupolosa analisi delle attività dei virus informatici consente all'azienda di offrire una protezione completa contro le minacce presenti e future. La resistenza agli attacchi futuri è la strategia di base implementata in tutti i prodotti Kaspersky Lab. L'azienda si trova costantemente all'avanguardia rispetto a numerosi altri produttori offrendo una protezione antivirus completa per utenti domestici e aziendali.

Anni di duro lavoro hanno fatto dell'azienda uno dei principali produttori di software per la sicurezza informatica. Kaspersky Lab è stata una delle prime aziende di questo tipo a sviluppare i più severi standard per la protezione antivirus. Il prodotto di punta dell'azienda, Kaspersky Anti-Virus, offre una protezione completa a tutti i livelli di una rete, inclusi workstation, file server, sistemi di posta elettronica, firewall, gateway Internet e palmari. I suoi strumenti di gestione, pratici e di facile utilizzo, garantiscono l'automazione avanzata per una sollecita protezione antivirus ad ogni livello dell'azienda. Numerose imprese di grande notorietà utilizzano Kaspersky Anti-Virus, tra cui Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India), BorderWare (Canada).

Gli utenti Kaspersky Lab possono usufruire di un'ampia gamma di servizi supplementari volti a garantire non solo un funzionamento stabile dei prodotti dell'azienda, ma anche la conformità a qualsiasi esigenza aziendale specifica. Il

database antivirus di Kaspersky Lab viene aggiornato ogni ora. L'azienda offre ai propri clienti un servizio di assistenza tecnica 24 ore su 24, disponibile in diverse lingue per soddisfare le esigenze di una clientela internazionale.

C.1. Altri prodotti Kaspersky Lab

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal è stato progettato per garantire la protezione antivirus dei personal computer con sistema operativo Windows 98/ME o Windows 2000/NT/XP contro tutti i virus conosciuti, compresi i software potenzialmente pericolosi. Kaspersky Anti-Virus Personal fornisce il monitoraggio in tempo reale di tutte le origini di intrusione dei virus - posta elettronica, Internet, dischi floppy, CD, ecc. L'esclusivo sistema di analisi euristica dei dati consente un'efficiente neutralizzazione dei virus ancora sconosciuti. Questa applicazione può operare nelle seguenti modalità (che possono essere utilizzate separatamente o congiuntamente):

- **Protezione del computer in tempo reale** - scansione antivirus di tutti gli oggetti eseguiti, aperti o salvati sul computer dell'utente.
- **Scansione manuale del computer**- scansione e disinfezione completa del computer o di singoli dischi, file e singole cartelle. Tale scansione può essere avviata manualmente, oppure è possibile pianificarne l'esecuzione automatica.

Kaspersky Anti-Virus® Personal non riesamina gli oggetti che sono già stati esaminati durante una scansione precedente e da allora non sono stati modificati, non solo nella modalità di protezione in tempo reale ma anche durante una scansione manuale. Questa funzione **aumenta notevolmente la velocità di funzionamento del programma**.

L'applicazione costituisce un'affidabile barriera contro i virus quando cercano di introdursi nel computer tramite posta elettronica. Kaspersky Anti-Virus® Personal provvede automaticamente a esaminare e disinfettare tutti i messaggi di posta elettronica in arrivo ed in uscita tramite i protocolli POP3 e SMTP, e garantisce un rilevamento molto efficiente dei virus nei database di posta.

L'applicazione supporta oltre 700 formati di archivi e file compressi ed è in grado di esaminarne automaticamente il contenuto, nonché di eliminare il codice ostile da archivi **ZIP, CAB, RAR**, **ARJ**, **LHA** e **ICE**.

La configurazione dell'applicazione e semplice ed intuitiva, grazie alla possibilità di selezionare uno dei tre livelli di protezione predefiniti: **Protezione massima**, **Raccomandato** o **Alta velocità**.

Il database antivirus viene aggiornato ogni ora, e l'invio dell'aggiornamento al computer dell'utente è garantito anche quando il computer è temporaneamente scollegato da Internet o è necessario cambiare connessione.

Kaspersky Anti-Virus® Personal Pro

Questo pacchetto è stato progettato per offrire una protezione antivirus completa ai computer domestici con sistema operativo Windows 98/ME, Windows 2000/NT, Microsoft Windows XP e le applicazioni di MS Office. Kaspersky Anti-Virus® Personal Pro include un'applicazione di facile utilizzo per il prelievo automatico degli aggiornamenti quotidiani del database antivirus e dei moduli dell'applicazione. L'esclusivo sistema di analisi euristica di seconda generazione rileva con efficacia i virus ignoti. L'interfaccia semplice e pratica consente agli utenti di configurare rapidamente il programma, rendendone l'utilizzo più facile che mai.

Kaspersky Anti-Virus® Personal Pro offre le seguenti funzioni:

- **Scansione manuale** dei dischi locali.
- **Protezione in tempo reale automatica** contro i virus di tutti i file ai quali si accede.
- Il **Filtro posta** esamina automaticamente e disinfetta tutti i messaggi in entrata e in uscita tramite i protocolli POP3 e SMTP e rileva con efficacia i virus nei database di posta.
- **Behavior blocker** garantisce la massima protezione delle applicazioni di MS Office contro i virus.
- **Scansione degli archivi** - Kaspersky Anti-Virus riconosce oltre 900 formati di archivi e file compressi, e garantisce la scansione antivirus automatica del loro contenuto e la rimozione del codice ostile dai file negli archivi **ZIP**, **CAB**, **RAR**, **ARJ**, **LHA** e **ICE**.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker è un firewall personale progettato per protegger un computer con qualsiasi sistema operativo Windows. Protegge il computer dagli accessi non autorizzati e gli attacchi dei pirati informatici, provenienti sia da Internet che dalla rete locale.

Kaspersky® Anti-Hacker controlla l'attività TCP/IP di rete di tutte le applicazioni eseguite sul computer. Quando rileva un'azione sospetta, Kaspersky® Anti-Hacker blocca l'accesso alla rete dell'applicazione sospetta. Questa misura consente all'utente di aumentare la privacy e conservare con tranquillità dati riservati nel proprio computer.

La tecnologia SmartStealth™ impedisce ai pirati informatici di rilevare il computer dall'esterno. In questa modalità, l'applicazione lavora ininterrottamente per

proteggere il computer mentre è sul Web: l'applicazione garantisce comunque la consueta trasparenza e accessibilità dei dati su Internet.

Kaspersky® Anti-Hacker blocca inoltre i più comuni attacchi dei pirati informatici e monitora costantemente i tentativi di scansione delle porte del computer.

La configurazione dell'applicazione prevede semplicemente la scelta di uno dei cinque livelli di sicurezza disponibili. Per impostazione predefinita, l'applicazione si avvia in modalità di autoapprendimento, che configura automaticamente il sistema di sicurezza in base alle risposte dell'utente a eventi di vario tipo. Questa caratteristica consente di personalizzare il programma in base alle preferenze ed esigenze specifiche dell'utente.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite è una suite software progettata per organizzare la protezione completa dei computer con sistema operativo Microsoft Windows. Questa suite previene la penetrazione dei programmi nocivi e potenzialmente pericolosi attraverso qualsiasi possibile origine dei dati, e protegge il computer dai tentativi non autorizzati di accedere ai dati, nonché dai messaggi di spam.

Kaspersky Personal Security Suite offre le seguenti funzioni:

- protezione antivirus dei dati salvati sul computer
- protezione contro i messaggi spam per gli utenti di Microsoft Outlook e Microsoft Outlook Express
- protezione del computer da accessi non autorizzati, nonché dagli attacchi dei pirati informatici dalla rete locale o da Internet.

Kaspersky Lab News Agent

Il News Agent è progettato per una rapida consegna di notizie pubblicate da Kaspersky Lab, di notifiche sullo stato corrente dell'attività dei virus e di notizie fresche. Il programma legge l'elenco dei canali di news disponibili ed il loro contenuto dai news server di Kaspersky Lab con una frequenza specificata.

Il prodotto offre le seguenti funzioni:

- Visualizza nell'area di notifica lo stato corrente delle attività dei virus.
- Il prodotto consente agli utenti di iscriversi ai canali di news o di annullare l'iscrizione.
- Recupera le notizie da ciascun canale al quale si sia effettuata l'iscrizione con la frequenza specificata, e notifica la presenza di notizie fresche.
- Consente di rivedere le notizie sui canali ai quali si sia effettuata l'iscrizione.
- Consente di rivedere l'elenco dei canali ed il loro stato.

- Consente di aprire pagine con notizie dettagliate nel browser.

News Agent è un'applicazione autonoma di Windows, che può essere utilizzata indipendentemente o in congiunzione con diverse soluzioni integrate offerte da Kaspersky Lab Ltd.

Kaspersky® On-Line Scanner

Il programma è un servizio gratuito offerto ai visitatori del sito Web di Kaspersky Lab. Il servizio consente un efficiente controllo antivirus on-line del computer. Kaspersky On-Line Scanner viene eseguito all'interno del browser Web tramite la tecnologia Microsoft ActiveX® . Questo servizio consente agli utenti di controllare rapidamente il proprio computer se si sospettano infezioni virali. Questo servizio consente agli utenti di:

- Escludere gli archivi e i database di posta dalla scansione.
- Selezionare il database antivirus standard/esteso per la scansione.
- Salvare un report sui risultati della scansione in formato txt o html.

Kaspersky® Security for PDA

Kaspersky® Security for PDA garantisce un'affidabile protezione antivirus dei dati salvati su diversi tipi di computer palmari e smartphone. Il programma comprende un set ottimale di strumenti di difesa antivirus:

- **scanner antivirus**, che esamina le informazioni (salvate sia nella memoria interna dei dispositivi PDA e smartphone o sulle memory card di qualsiasi tipo) su richiesta dell'utente;
- **monitor antivirus** per intercettare i virus nei file che vengono copiati da altri dispositivi palmari o trasferiti tramite la tecnologia HotSync™.

Kaspersky® Security for PDA protegge i dispositivi palmari (PDA) dall'accesso non autorizzato criptando l'accesso al dispositivo stesso e ai dati memorizzati sulle memory card.

Kaspersky Anti-Virus® Business Optimal

Il pacchetto è stato sviluppato per garantire un'esclusiva soluzione di sicurezza per reti aziendali di piccole e medie dimensioni.

Kaspersky Anti-Virus® Business Optimal garantisce la protezione antivirus completa[4] di:

- *Workstation* con sistema operativo Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation e Linux.

[4] A seconda del tipo di kit di distribuzione.

- *File server* con sistema operativo Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD e OpenBSD, Linux, Samba Servers.
- *Sistemi di posta elettronica* tra cui Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, e Qmail.
- *Gateway Internet*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

Il kit di distribuzione di Kaspersky Anti-Virus® Business Optimal comprende Kaspersky® Administration Kit, uno strumento esclusivo per la gestione e l'amministrazione automatizzate.

La vasta gamma di applicazioni antivirus disponibili offre la massima libertà di scelta in base al sistema operativo e alle applicazioni in uso.

Kaspersky® Corporate Suite

Questo pacchetto è stato sviluppato per offrire una protezione antivirus completa e scalabile alle reti aziendali di qualsiasi dimensione e complessità. I componenti del pacchetto garantiscono la protezione di tutti i livelli di una rete aziendale, anche in ambienti informatici misti. Kaspersky® Corporate Suite supporta la maggior parte dei sistemi operativi e delle applicazioni in uso nelle aziende. Tutti i componenti del pacchetto sono gestiti da una consolle mediante un'unica interfaccia utente. Kaspersky® Corporate Suite è un affidabile sistema di protezione di alto livello totalmente compatibile con le esigenze specifiche di ogni configurazione di rete.

Kaspersky® Corporate Suite include la protezione antivirus completa per:

- *Workstation* con sistema operativo Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation e Linux;
- *File server* con sistema operativo Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux e Samba Servers;
- *Sistemi di posta elettronica* tra cui Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim e Qmail;
- *Gateway Internet*: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition;
- *Computer palmari* (PDA), con sistema operativo Windows CE e Palm OS, nonché smartphone con sistema operativo Windows Mobile 2003 for Smartphone e Microsoft Smartphone 2002.

Il kit di distribuzione di Kaspersky® Corporate Suite comprende Kaspersky® Administration Kit, uno strumento *esclusivo per la gestione e l'amministrazione automatizzate.*

La vasta gamma di applicazioni antivirus disponibili offre la massima libertà di scelta in base al sistema operativo e alle applicazioni in uso.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam è un'innovativa suite di software progettata per assistere le aziende con reti di piccole e medie dimensioni nella difesa contro i sempre più numerosi messaggi di posta elettronica non desiderati (spam). Il prodotto combina la rivoluzionaria tecnologia di analisi linguistica con metodi moderni di filtraggio della posta elettronica, tra cui gli elenchi RBL e le caratteristiche delle lettere formali. L'esclusiva combinazione di servizi consente agli utenti di identificare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, Kaspersky® Anti-Spam è una barriera alla posta non desiderata controllando tutta la posta in entrata alla ricerca di spam. Il software è compatibile con qualsiasi sistema di posta e può essere installato sia su server mail esistenti, sia su server dedicati.

L'elevato grado di efficacia di Kaspersky® Anti-Spam è garantito dall'aggiornamento quotidiano del database di filtraggio dei contenuti con i campioni forniti dagli specialisti del laboratorio linguistico dell'azienda. I database vengono aggiornati ogni 20 minuti.

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix è una soluzione progettata per l'elaborazione antivirus della posta elettronica inviata attraverso il protocollo SMTP. Quest'applicazione contiene numerosi strumenti supplementari per il filtraggio del traffico di posta elettronica in base al nome e il tipo di allegati MIME, riducendo il carico sul sistema di posta elettronica e prevenendo gli attacchi dei pirati informatici. Il supporto per DNS Black List garantisce la protezione dai messaggi di posta elettronica provenienti da server compresi in tali elenchi come origini di posta indesiderata (spam).

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange effettua l'elaborazione antivirus dei messaggi di posta elettronica in arrivo ed in uscita, come anche di tutti i messaggi archiviati sul server, compresi i messaggi nelle cartelle pubbliche, e filtra la corrispondenza non desiderata utilizzando tecniche "intelligenti" di riconoscimento spam in combinazione con le tecnologie Microsoft. L'applicazione esamina tutti i messaggi ricevuti su un Exchange Server tramite il protocollo SMTP controllandoli alla ricerca di attributi SPAM e virus tramite le tecnologie antivirus di Kaspersky Lab. Filtra i messaggi spam sulla base degli attributi formali (indirizzo di posta elettronica, indirizzo IP, dimensione del messaggio,

intestazione) ed analizza il contenuto dei messaggi e dei loro allegati utilizzando tecnologie "intelligenti", tra cui le firme grafiche esclusive, per identificare SPAM grafiche. L'applicazione esamina il corpo del messaggio ed i file allegati.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway è una soluzione completa che fornisce la protezione totale per gli utenti di sistemi di posta elettronica. Questa applicazione, installata tra la rete aziendale e Internet, esamina tutti i componenti dei messaggi di posta elettronica alla ricerca di virus ed altri malware (spyware, adware, ecc.), ed esegue il filtraggio centralizzato anti-spam dei flussi di posta elettronica. Questa soluzione comprende inoltre alcune caratteristiche supplementari di filtraggio del traffico di posta elettronica.

C.2. Recapiti

Per domande, commenti e suggerimenti, rivolgetevi a un nostro distributore o direttamente a Kaspersky Lab. Saremo lieti di aiutarvi per qualsiasi questione legata ai nostri prodotti, per telefono o via posta elettronica. Tutte le raccomandazioni e i suggerimenti pervenuti saranno presi in considerazione e valutati con attenzione.

Assistenza tecnica	Per qualsiasi informazione relativa all'assistenza tecnica, visitare la pagina http://www.kaspersky.com/supportinter.html
Informazioni generali	WWW: http://www.kaspersky.com http://www.viruslist.com Posta elettronica: sales@kaspersky.com

APPENDICE D. CONTRATTO DI LICENZA

Contratto di licenza per l'utente finale

AVVERTENZA PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO LEGALMENTE VINCOLANTE ("CONTRATTO") RELATIVO AL SOFTWARE SPECIFICATO ("SOFTWARE") PRODOTTO DA KASPERSKY LAB ("KASPERSKY LAB").

QUANDO ACQUISTA IL PRESENTE SOFTWARE VIA INTERNET, FACENDO CLIC SUL PULSANTE DI ACCETTAZIONE, L'UTENTE ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO E A DIVENTARNE UNA DELLE PARTI. IN CASO CONTRARIO, FACENDO CLIC SUL PULSANTE CHE INDICA LA MANCATA ACCETTAZIONE DI TUTTE LE CONDIZIONI DEL PRESENTE, L'UTENTE RINUNCIA A INSTALLARE IL SOFTWARE.

SE IL SOFTWARE È STATO ACQUISTATO SU SUPPORTO FISICO E L'UTENTE HA ROTTO IL SIGILLO DELLA BUSTA DEL CD, ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO. SE L'UTENTE NON ACCETTA TUTTE LE CONDIZIONI DEL PRESENTE CONTRATTO, EGLI DOVRÀ ASTENERSI DAL ROMPERE IL SIGILLO DELLA BUSTA DEL CD, SCARICARE, INSTALLARE O UTILIZZARE QUESTO SOFTWARE.

CONFORMEMENTE ALLA NORMATIVA RELATIVA AL SOFTWARE KASPERSKY PER SINGOLI UTENTI (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) ACQUISTATO SCARICANDO IL FILE DAL SITO WEB DI KASPERSKY LAB, IL CLIENTE PUÒ RESTITUIRE IL PRODOTTO AL RIVENDITORE PER LA SOSTITUZIONE O IL RIMBORSO COMPLETO ENTRO 7 GIORNI LAVORATIVI DALLA DATA DELL'ACQUISTO, A PATTO CHE IL SIGILLO NON SIA STATO ROTTO..

IL SOFTWARE PER UTENTI SINGOLI (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) NON ACQUISTATO ONLINE SU INTERNET NON PUÒ ESSERE

RESTITUITO PER IL RIMBORSO NÉ PER LA SOSTITUZIONE SE NON DIVERSAMENTE STABILITO DAL PARTNER CHE RIVENDE IL PRODOTTO. IN QUESTO CASO, KASPERSKY LAB NON È VINCOLATO DALLE CLAUSOLE STABILITE DAL PARTNER.

IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SPETTA SOLO ALL'ACQUIRENTE ORIGINARIO.

Tutti i riferimenti al termine "Software" contenuti nel presente documento includeranno la chiave di attivazione software ("File di identificazione chiave") che sarà fornita all'utente da Kaspersky Lab come parte integrante del Software.

1. Concessione della licenza. Previo pagamento delle tasse di licenza applicabili e nel rispetto dei termini e delle condizioni del presente Contratto, con il presente Kaspersky Lab concede all'utente il diritto non esclusivo e non trasferibile di utilizzare una copia della versione specificata del Software e la documentazione in accompagnamento (la "Documentazione") per la durata del presente Contratto e unicamente a uso aziendale interno. È possibile installare una copia del software su un computer, una workstation, un palmare o un altro dispositivo elettronico per cui è stato progettato il Software (ciascuno dei quali denominato "Dispositivo client"). Se il Software è concesso su licenza come suite o pacchetto contenente più di un prodotto Software specificato, tale licenza si applica a tutti i prodotti software specificati, ed è soggetta alle restrizioni o alle condizioni d'uso specificate sul listino prezzi applicabile o sull'imballo di ciascun singolo prodotto Software.

1.1 Uso. Il Software è concesso in licenza in qualità di singolo prodotto; non può essere utilizzato su più di un Dispositivo client o da più di un utente per volta, salvo quanto diversamente specificato nella presente Sezione.

1.1.1 Il Software è "in uso" su un Dispositivo client quando è caricato nella memoria temporanea (vale a dire nella memoria ad accesso casuale o RAM) o è installato nella memoria permanente (per esempio disco fisso, CD-ROM, o altro dispositivo di memoria) di quel dispositivo client. La presente licenza autorizza l'utente a creare il numero di copie di backup del Software necessarie per il suo utilizzo legale e unicamente a scopi di archivio, a condizione che tutte le copie contengano le informazioni di proprietà del software. L'utente è tenuto a mantenere traccia del numero e dell'ubicazione di tutte le copie del Software e della Documentazione e a prendere tutte le ragionevoli precauzioni per proteggere il Software da copia o utilizzo non autorizzati.

1.1.2 Qualora l'utente venda il Dispositivo client su cui è installato il Software, dovrà assicurarsi che tutte le copie del Software siano state cancellate.

1.1.3 All'utente è fatto divieto di decompilare, reverse engineer, disassemblare o altrimenti ridurre qualsiasi parte del presente Software a una forma leggibile dall'uomo e di permettere a terzi di compiere tali azioni. Le informazioni di interfaccia necessarie per ottenere l'interoperatività del software con programmi per computer creati indipendentemente sarà fornita da Kaspersky Lab dietro

richiesta e dietro pagamento dei ragionevoli costi e delle spese sostenute per procurarsi e fornire tali informazioni. Qualora Kaspersky Lab notificasse al cliente che, per qualsiasi ragione, inclusa senza tuttavia ad essa limitarsi quella dei costi, non intende fornire tali informazioni, l'utente sarà autorizzato a intraprendere le azioni necessarie per ottenere l'interoperatività a condizione di eseguire le operazioni di decompilazione o reverse engineering entro i limiti previsti dalla legge.

1.1.4 L'utente non deve né deve permettere ad altri (in modo diverso da quanto espressamente permesso nel presente documento) di effettuare la correzione di errori o altrimenti modificare, adattare o tradurre il Software né creare opere derivate dal Software.

1.1.5 All'utente è fatto divieto di affittare, noleggiare o prestare il Software a terzi oltre che di trasferire o di fornire a terzi la licenza in concessione.

1.1.6 All'utente è fatto divieto di utilizzare il Software con strumenti automatici, semi-automatici o manuali progettati per creare firme virus, routine di rilevazione virus, qualsiasi altro dato o codice per la rilevazione di codici o dati maligni.

1.2 Utilizzo in modalità Server. L'utente può utilizzare il Software su un Dispositivo Client o su un server o un dispositivo che operi come tale ("Server") nell'ambito di un ambiente multiutente o collegato in rete ("Modalità Server") solo se tale uso è consentito dal listino prezzi applicabile o sull'imballo del Software. È richiesta una licenza separata per ogni Dispositivo Client o postazione dalla quale ci si connette al Server, indipendentemente dal fatto che tali dispositivi Client o postazioni concesse in licenza si connettano contemporaneamente o stiano effettivamente accedendo al Software o utilizzando lo stesso. L'utilizzo di software o hardware che riduce il numero di Dispositivi Client o postazioni con utilizzo o accesso diretto al Software (per esempio software o hardware di "multiplexing" o "pooling") non riduce il numero di licenze richieste (in quanto il numero richiesto di licenze sarebbe pari al numero di ingressi distinti al software o hardware di multiplexing o pooling "front end"). Se il numero di Dispositivi Client o di postazioni che possono connettersi al Software è maggiore del numero di licenze ottenute, l'utente deve disporre di un meccanismo ragionevole che garantisca che l'uso del Software non supera i limiti di utilizzo specificati per la licenza ottenuta. La presente licenza autorizza l'utente a effettuare o scaricare il numero di copie della Documentazione per ogni Dispositivo Client o postazione concessi in licenza necessario per il suo utilizzo ai termini di legge, a condizione che ogni copia contenga tutte le informazioni sui diritti di proprietà della Documentazione.

1.3 Licenze per volume. Se il Software è concesso dietro una licenza per volume le cui condizioni sono specificate nella fattura applicabile del prodotto o sull'imballo del Software, l'utente può effettuare, utilizzare o installare tante copie supplementari del software sul numero di Dispositivi Client quante sono specificate nelle condizioni della licenza per volume. L'utente deve applicare meccanismi ragionevoli per garantire che il numero di Dispositivi Client su cui è

stato installato il Software non superi il numero di licenze ottenute. La presente licenza autorizza l'utente a effettuare o scaricare una copia della Documentazione per ogni copia supplementare autorizzata dalla licenza per volume, a condizione che ogni copia contenga tutte le informazioni sui diritti di proprietà della Documentazione.

2. Durata. Il presente Contratto è valido per il periodo specificato nel file chiave (il file esclusivo necessario per abilitare completamente il Software; vedere la Guida/Informazioni sul Software; per la versione Unix/Linux del Software vedere l'avviso sulla data di scadenza del file chiave) salvo risoluzione anticipata e in tal caso fino alla data di tale risoluzione, come esposto nel presente documento. Il presente Contratto terminerà automaticamente in caso di mancata osservanza da parte dell'utente di una delle condizioni, limitazioni o altri requisiti descritti nel presente. Al momento della rescissione o alla scadenza del presente Contratto, l'utente è tenuto a distruggere immediatamente tutte le copie del Software e della Documentazione. È possibile recedere dal presente Contratto in qualsiasi momento distruggendo tutte le copie del Software e della Documentazione.

3. Assistenza.

(i) Kaspersky Lab fornirà al cliente i servizi di assistenza ("Servizi di assistenza") di seguito definiti per un periodo di un anno dietro:

(a) pagamento della tariffa di assistenza corrente; e

(b) compilazione del Modulo di richiesta dei Servizi di assistenza fornito in allegato al presente Contratto o disponibile nel sito web di Kaspersky Lab, nel quale si richiede all'utente di fornire il proprio File di identificazione chiave fornito all'utente da Kaspersky Lab con il presente Contratto. Kaspersky Lab ha il diritto di stabilire, a propria discrezione, se l'utente abbia soddisfatto o meno questa condizione per la fornitura dei Servizi di Assistenza.

(ii) I Servizi di Assistenza termineranno alla scadenza, salvo rinnovo annuo dietro il pagamento della tariffa annuale corrente e dietro soddisfacente nuova compilazione del Modulo di sottoscrizione ai servizi di assistenza .

(iii) Con la compilazione del Modulo di sottoscrizione ai servizi di assistenza, l'utente accetta i termini della politica di tutela della riservatezza adottata da Kaspersky Lab, consultabile su www.kaspersky.com/privacy, e acconsente esplicitamente al trasferimento dei propri dati in paesi esterni a quello di residenza, come specificato nella politica di tutela della riservatezza.

(iv) Per "Servizi di assistenza" si intende

(a) Aggiornamenti quotidiani gratuiti del database antivirus;

(b) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione;

(c) Assistenza tecnica estesa tramite posta elettronica o linea telefonica dedicata forniti dal distributore e/o dal rivenditore;

(d) Aggiornamenti per la rilevazione e la disinfezione dei virus 24 ore su 24.

4. Diritti di proprietà. Il Software è protetto dalle leggi sul copyright. Kaspersky Lab e i relativi fornitori possiedono e mantengono tutti i diritti, l'autorità e gli interessi del Software e ad esso correlati, inclusi tutti i diritti di proprietà, i brevetti, i marchi commerciali e gli altri diritti di proprietà intellettuale ad esso connessi. Il possesso, l'installazione o l'utilizzo del Software non trasferiscono all'utente alcun diritto relativo alla proprietà intellettuale del Software e non determinano l'acquisizione di diritti sul Software salvo quelli espressamente indicati nel presente Contratto.

5. Riservatezza. L'utente riconosce che il Software e la Documentazione, inclusa la specifica configurazione e la struttura dei singoli programmi e il File di identificazione chiave costituiscono informazioni proprietarie riservate di Kaspersky Lab. L'utente non dovrà divulgare, fornire o altrimenti rendere disponibili tali informazioni riservate in qualsivoglia forma a terzi senza previo consenso scritto di Kaspersky Lab. Dovrà inoltre applicare ragionevoli misure di sicurezza volte a proteggere tali informazioni riservate ma, senza tuttavia limitarsi a quanto sopra espresso dovrà fare quanto in suo potere per tutelare la sicurezza del File di identificazione chiave.

6. Garanzia limitata

(i) Kaspersky Lab garantisce che per un periodo di sei (6) mesi a decorrere dal prelievo o installazione il Software acquistato su supporto fisico opererà sostanzialmente in conformità alle funzioni descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione.

(ii) L'utente si assume ogni responsabilità in merito alla scelta del presente Software per le proprie esigenze. Kaspersky Lab non garantisce che il Software e/o la Documentazione siano idonei a soddisfare le esigenze dell'utente né che il suo utilizzo sia esente da interruzioni o privo di errori.

(iii) Kaspersky Lab non garantisce che il Software identifichi tutti i virus noti né esclude che possa occasionalmente eseguire il report erroneo di un virus in un titolo non infettato da quel virus.

(iv) L'indennizzo dell'utente e la completa responsabilità di Kaspersky Lab per la violazione della garanzia di cui al paragrafo (i) saranno a discrezione di Kaspersky Lab, che deciderà se riparare, sostituire o rimborsare il Software in caso di reclamo a Kaspersky Lab o suoi fornitori durante il periodo di garanzia. L'utente dovrà fornire tutte le informazioni ragionevolmente necessarie per agevolare il Fornitore nel ripristino dell'articolo difettoso.

(v) La garanzia di cui al punto (i) non è applicabile qualora l'utente (a) apporti modifiche al presente Software o determini la necessità di modificarlo senza il consenso di Kaspersky Lab, (b) utilizzi il Software in modo difforme dall'uso previsto o (c) impieghi il Software per usi diversi da quelli permessi ai sensi del presente Contratto.

(vi) Le garanzie e le condizioni specificate in questo Contratto sostituiscono qualsiasi altra condizione, garanzia o termine relativi alla fornitura o alla presunta fornitura, all'impossibilità di fornire o al ritardo nella fornitura del Software o della Documentazione che, se non fosse per questo paragrafo (v), potrebbero verificarsi tra Kaspersky Lab e voi o sarebbero altrimenti impliciti o incorporati nel presente Contratto o in qualsiasi altro contratto collaterale, per disposizione statutaria, legislazione vigente o altro, che con ciò sarebbero esclusi (inclusi, senza limitazione, le condizioni implicite, le garanzie o altri termini relativi all'adeguatezza della qualità, all'idoneità allo scopo o all'uso di competenza e cura ragionevoli).

7. Limitazione di responsabilità

(i) Nessun elemento nel presente Contratto deve escludere o limitare la responsabilità di Kaspersky Lab relativamente a (a) responsabilità civile per frode, (b) decesso o lesioni personali causate da un suo mancato esercizio di cautela ai sensi del diritto consuetudinario o (c) dalla violazione negligente di una delle condizioni del presente Contratto.

(ii) Ai sensi del paragrafo (i), il Fornitore non deve essere ritenuto responsabile (relativamente al contratto, per responsabilità civile, restituzione o altro) per i seguenti danni o perdite (siano questi danni o perdite previsti, prevedibili, noti o altro):

(a) perdita di reddito;

(b) perdita di utili effettivi o presunti (inclusa la perdita di utili sui contratti);

(c) perdita di liquidità;

(d) perdita di risparmi presunti;

(e) perdita di affari;

(f) perdita di opportunità;

(g) perdita di avviamento;

(h) danni alla reputazione;

(i) perdita, danni o corruzione di dati; o

(j) eventuali perdite indirette o conseguenti o danni arrecati in qualsiasi modo (inclusi, a scanso di dubbi, i danni o le perdite del tipo specificato nei paragrafi (ii), da (a) a (ii), (i).

(iii) Ai sensi del paragrafo (i), la responsabilità di Kaspersky Lab (né a fini del contratto, frode, restituzione o in nessun'altra maniera) derivante da o in relazione alla fornitura del Software non supererà in nessun caso l'importo corrispondente all'onere ugualmente sostenuto dall'utente per il Software.

8. (i) Il presente Contratto contiene per intero tutti gli intendimenti delle parti relativamente all'oggetto del presente e sostituisce tutti gli eventuali accordi,

impegni e promesse precedenti tra l'utente e Kaspersky Lab, sia orali che per iscritto, che possano scaturire o essere impliciti da qualsiasi cosa scritta o pronunciata oralmente in fase di negoziazione tra Kaspersky Lab o suoi rappresentanti e l'utente precedentemente al presente Contratto; tutti gli accordi precedenti tra le parti relativamente all'oggetto di cui sopra decadranno a partire dalla Data di entrata in vigore del presente Contratto. Fatto salvo quanto stabilito ai paragrafi (ii) - (iii) di seguito, l'utente non sarà in alcun modo risarcito per eventuali false dichiarazioni ricevute sulle quali aveva fatto affidamento nella stipula del presente Contratto ("Falsa dichiarazione") e Kaspersky Lab non sarà vincolata da altre responsabilità oltre a quelle relative alle espresse condizioni del presente Contratto.

(ii) Nessun elemento del presente Contratto deve escludere o limitare la responsabilità di Kaspersky Lab relativamente ad eventuali dichiarazioni erronee in esso presenti se rese in malafede.

(iii) La responsabilità di Kaspersky Lab per eventuali false dichiarazioni relativamente ad aspetti fondamentali, incluso un aspetto fondamentale relativo alla capacità del fabbricante di adempiere ai propri obblighi ai sensi del presente Contratto, sarà soggetta alla clausola di responsabilità limitata di cui al paragrafo 7 (iii).